

CA Service Catalog

Implementation Guide

Release 12.7.00



This documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the "Documentation") is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

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

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

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

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

The manufacturer of this Documentation is CA.

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

Copyright © 2011 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

CA Technologies Product References

This documentation set contains references to the following CA Technologies products:

- CA Service Catalog, which includes CA Service Accounting
- CA Embedded Entitlements Manager (CA EEM)
- CA Automation Suites (formerly CA Spectrum Automation Manager)
- CA Automation Suites Reservation Manager (Reservation Manager)
- CA Business Service Insight (CA BSI, formerly CA Oblicore Guarantee)
- CA Service Desk Manager, which includes CA CMDB
- CA SiteMinder®
- CA Asset Portfolio Management (CA APM)
- CA MICS® Resource Management
- CA JARS®
- CA Storage Resource Manager (CA SRM)
- CA Workflow
- CA Process Automation (formerly CA IT PAM)
- CA Business Intelligence
- CA Anti-Virus (formerly eTrust Antivirus)
- CA Threat Manager (formerly eTrust Integrated Threat Management [eTrust ITM])

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

If you would like to provide feedback about CA Technologies product documentation, complete our short customer survey, which is available on the CA Support website at <http://ca.com/docs>.

Contents

Chapter 1: Planning	13
How to Plan Your Implementation	13
Business Processes	13
System Architecture	14
Demonstration-Only Deployment	14
Key Terms and Concepts	14
Small Architecture	15
Medium Architecture	16
Large Architecture	17
Failover Mechanisms	18
Session Management	19
Scenario	19
Clustering	21
Authentication Methods	21
Products and Components Overview	22
Overview of Integrations	23
Integrations Supplied on the CA Service Catalog Installation Media	23
Integrations Supplied in Addition to the CA Service Catalog Installation Media	24
Integrations Supplied Separately	25
Chapter 2: Preparing to Install or Upgrade	27
New Installation, Upgrade, or Migration	27
Considerations and Requirements Before Installation	28
Release Notes	28
Operating System	29
Operating System Language	29
Web Application Servers	29
System Requirements and Related Requirements	29
Requirements and Considerations for the DBMS and CA MDB	32
Authentication and Authorization	35
Host Names and Port Numbers	35
Server Architecture	36
Service Provider Business Unit ID	37
Chapter 3: Installing	39
How to Install	40

CA EEM Installation Considerations	41
Install CA EEM	41
How to Prepare for the MDB Installation or Upgrade	42
Parameters for MDB on SQL Server	43
Parameters for MDB on Oracle	44
Install Service View	46
Install CA Service Catalog	48
Installation of a Process Automation Tool	49
Install CA Workflow	49
Install Catalog Content	51
Install CA Service Accounting	52
Installation and Configuration Procedures for Third-Party Unicode Fonts	53

Chapter 4: Upgrading 55

Traditional and Migration Model Upgrades	55
Scope and Limitations of an Upgrade	56
Prepare for the Upgrade	57
Prepare the MDB and the DBMS	59
Back Up CA EEM Data	60
How to Upgrade Using a Migration Model	61
Guidelines for Migration Model Upgrades	62
How to Install CA Service Catalog Products and Components	62
How to Upgrade Using a Traditional Model	63
Upgrade CA EEM	64
Upgrade Service View and Other Products and Components	65
Finalize the Upgrade	68
How to Set Up Shared and Customized Files	69
Configure CA Workflow	71

Chapter 5: Migrating 73

Migration	73
Disaster Recovery	74
How to Perform Prerequisite Tasks	74
How to Migrate	75

Chapter 6: Content Packs 79

Overview of Content Packs	79
How to Manage Content Packs	80
Export Content Packs	81
Import Content Packs	84

Actions that You Can Perform on Imported Objects.....	85
Enable and Disable Content Packs	87

Chapter 7: Content Configuration Form 91

Overview of Content Configuration Form.....	91
Create the Content Configuration Form	92
Retrieve Values from Fields on Content Configuration Forms.....	94

Chapter 8: Configuring 97

Integrations	97
Obtain Product License Keys	98
Service Delivery Administrator.....	98
Assign the Service Delivery Administrator Role to a User.....	99
Change Your Password.....	100
Verify that Browser Security Settings Permit Login	101
How to Enhance Security	102
Required Open Ports	103
How to Enable External Authentication of Users.....	104
Configure NTLM Authentication on Windows	105
Configure Single Sign-on Type Setting for External Authentication.....	106
How to Configure CA Service Catalog to Use Secure Socket Layer	106
Create a Keystore File	108
Merge Keystore Files.....	109
Configure Service View to Use Secure Socket Layer	110
Configure CA Workflow to Use Secure Socket Layer	111
Edit the Server.xml File to Support SSL	112
Configure CA Workflow to Communicate with CA Service Catalog Using Secure Socket Layer	113
Configure CA IT PAM to Communicate with CA Service Catalog Using Secure Socket Layer	114
Configure BusinessObjects Enterprise to Communicate with CA Service Catalog Using Secure Socket Layer.....	115
Add Self-Signed Certificates to the Keystore	116
How to Verify Configuration Settings.....	117
Inheritance of Configuration Settings Through the Business Unit Hierarchy	118
Administration Configuration Options	119
Set Administration Configuration Options.....	119
How to Manage Fiscal Periods	135
Verify the Product License	137
Accounting Configuration Options	138
Change the Business Unit.....	139
Set Accounting Configuration Options.....	139
Manage Subscriptions.....	161

Exchange Rates	164
Manage Exchange Rates	164
Set Service Builder Configuration Options	169
Change the Business Unit.....	171
Catalog Configuration Options.....	172
Request Management Configuration Options	173
System Configuration.....	185
Configuration of Web Services.....	186
Single Location for Shared Files.....	186
Set Up a Single Location for Shared Files	187
Perform the Prerequisite Tasks.....	188
Advantages of 64-Bit Mode.....	189
Configure Components to Run in 64-Bit or 32-Bit Mode	189
Updates Made by the Ant Command.....	191

Chapter 9: Maintenance 193

Files to Back Up Regularly	193
CA Management Database.....	194
Update the Password of the Database User	194
Update the Database Host, Port, Instance, or Service Names	196
Update the CA EEM Host Name and Application Names.....	198
Update the Host Name and Port Number for Service View and CA Workflow	202
How to Maintain Log Files.....	204
Names and Locations of All Log Files	205
Most Frequently Used Log Files	207
How to Set Log Levels	210
Log Files Controlled by Each Log4j.xml File.....	211
Set the Log Level of a Service.....	212
Configure Rollover Settings for Selected Log Files	213

Chapter 10: Clustering 215

How to Implement Clustering	215
Perform the Preliminary Tasks	216
Meet the Prerequisites.....	217
How to Set Up Vertical Clustering for Service View	218
Perform the Initial Setup.....	219
Set Up Each Additional Cluster.....	220
Updates Made Automatically When You Set Up a Cluster	222
Verify the Server.xml Files.....	225
Remove a Cluster	226
Set Up Horizontal Clustering for Service View	228

Remove a Cluster	230
Set Up NTLM Authentication for Each Cluster	230
Configure NTLM Authentication with Apache Load Balancer	231
Configure NTLM Authentication with Another Type of Load Balancer	232
Set Up Horizontal Clustering for CA Workflow	233
Remove a Cluster	235
How to Set Up Load Balancing	236
Configure Apache HTTP Server	236
Disable Web Server Features	237
How to Create and Configure the workers.properties File	238
Create the uriworkermap.properties File	246
Update the httpd.conf File	247
How to Verify Load Balancing	250

Chapter 11: Best Practices 253

Overview	253
Benefits	254
Guidelines for Collecting Data	255
Purpose of the Staff Interviews	255
Questions for Staff Interviews	256
Staff Interviews	256
Documents to Analyze	257
Review and Benchmark Activities	257
Results of Staff Interviews	258
Best Practices Foundation	258
Request and Fulfillment Automation with CA Workflow and CA Process Automation	258
Service Catalog Logical Structure	260
Customer-Focused Documentation	262
Guidelines for Customizing Catalog Content	263
Frequently Asked Questions	264
Catalog Entries	265
Service Specification	269

Chapter 12: Customizing 275

Introduction to Customization	275
How to Add Custom Fields to the User Interface	276
Additional Data Fields	276
Sample Custom.xml File	277
Expose Additional Data Fields	278
Request Status Values	279
How to Customize the Request Status List	280

Become Familiar with requestshared.xml	280
Add an Additional Request Status.....	286
Hide Request Statuses	289
Restrict the Status Changes Available for a Request Item Based on its Current Status.....	291
Category, Class and Subclass Lists.....	294
Customize the Category, Class and Subclass Lists.....	295
User and Service Approval List.....	297
Maintain the User and Service Approval Level List	298
Request and Priority List	299
Priority Levels.....	300
How to Maintain the Request Priority List.....	301
Typefaces Available for Notes in Requests	304
How to Customize the Typefaces Available for Notes in Requests.....	305
How to Customize XSL, XML, JavaScript, and Image Files.....	306
Increase the Number of Values for a Drop-Down Variable.....	308
Custom Branding.....	309
Upgrade Considerations.....	310
How to Customize Logos.....	311
Customization of the Login Page.....	314
Themes.....	320
Global Page Elements	327
Customize the Online Help.....	330

Chapter 13: Uninstalling 331

How to Uninstall CA Service Catalog.....	331
Uninstall CA Service Catalog Components	332

Appendix A: Troubleshooting 333

Scope.....	333
Cannot Log In to CA Service Catalog	334
Cannot Add or Update a User Because of Duplicate User ID	335
Cannot Delete an Account	336
Cannot Connect to a Trusted Computer	336
Cannot Email a Request	337
Cannot Locate the Configuration Files	337
Cannot Locate My Log Files.....	338
Compilation Errors After Customization	338
Log File Does Not Roll Over	338
Cannot Locate the Registry Keys.....	339
Cannot Set Debug Levels.....	340
Cannot Open Documents from the Web Folder	340

Message Queue 4.1 Broker Stops Immediately After Starting.....	340
Message Queue 4.1 Broker Does Not Respond to Scans	341
In HTTPS, Unable to View Invoice in CSV Format from Invoice History UI.....	342
IXUTIL Out-of-Memory Error Occurs	343
Pages Do Not Appear to Be Refreshing Properly	343
A Request Approval or Fulfillment Pending Action Is Not Assigned	343
Requests Are Assigned to Multiple Users and Groups.....	344
Requests Do Not Move to the Next Status	345
Sorting of Services by Selection Type.....	347
Service View Installation or Upgrade Fails Because Path Name is Too Long	347
Service View Installation or Upgrade Fails Because of Duplicate Records.....	348
Service View Windows Service Does Not Start	348
CA EEM Installation on 64-Bit Operating Systems	349
CA EEM Upgrade Fails	349

Chapter 1: Planning

This section contains the following topics:

[How to Plan Your Implementation](#) (see page 13)

[Business Processes](#) (see page 13)

[System Architecture](#) (see page 14)

[Clustering](#) (see page 21)

[Authentication Methods](#) (see page 21)

[Products and Components Overview](#) (see page 22)

[Overview of Integrations](#) (see page 23)

How to Plan Your Implementation

The CA Service Catalog products and components are an integrated set of business applications for managing services. These applications organize your operational data into modular business solutions, procedures, and functions that you can automate.

To plan your implementation of CA Service Catalog, follow this process:

1. Determine your [business processes](#) (see page 13).
2. Determine the [system architecture](#) (see page 14) to use.
3. Determine the [authentication method](#) (see page 21) or methods to use.
4. Decide which [products and components](#) (see page 22) to install.
5. Determine which CA products to [integrate](#) (see page 23) with CA Service Catalog and plan for the installation of those products.

After you plan your implementation, you prepare to install or upgrade CA Service Catalog.

Business Processes

Implementing CA Service Catalog requires an understanding of your current business processes. Often this effort requires a discovery process to research and obtain this information. During this process, you ask questions and collate information about your business processes. Use top-down analysis to define your business and your business needs. After you determine your business needs, implement the catalog system to address them.

System Architecture

In a production environment, CA Service Catalog supports the following types of system architecture:

- [Small Architecture](#) (see page 15)
- [Medium Architecture](#) (see page 16)
- [Large Architecture](#) (see page 17)

Demonstration-Only Deployment

In addition to small, medium, and large architectures, CA Service Catalog also supports a standalone deployment. In a standalone deployment, all the components, including the database server, are installed on a single physical computer. This deployment is for demonstration *only* and is *not* suitable for a production environment.

Key Terms and Concepts

Availability refers to the ability of an organization to deliver consistent, predictable access to applications and data.

The number of *catalog requests per minute* is the key criterion for determining the size of the architecture as [small](#) (see page 15), [medium](#) (see page 16), or [large](#) (see page 17). This criterion is much more important than the number of users in the system or other criteria. The higher the number of catalog requests per minute, the larger the recommended architecture.

A *cluster* is two or more interconnected computers that create a solution to provide higher availability, higher scalability, or both.

Clustering for CA Service Catalog and CA Service Accounting is accomplished through Service View clustering, because all user communications with catalog and accounting functions are accomplished through Service View. Thus, the term *Service View clustering* includes both CA Service Catalog clustering and CA Service Accounting clustering.

Load balancing means dividing the amount of work between two or more computers, instead of a single computer. As a result, the system accomplishes more work in the same amount of time and typically serves all users faster.

In *horizontal clustering*, different physical computers comprise a cluster. As a result, the load balancer forwards requests to different computers having different IP addresses. All Service View installations on all computers must use the same cluster of the MDB. To [implement clustering](#) (see page 215), you make several related configuration changes *manually*. Horizontal clustering enables a single application to span several computers while presenting a single system image. Horizontal clustering can also provide increased throughput and high availability. Horizontal clustering applies to *both* Service View and CA Workflow.

In *vertical clustering*, all servers are on the same computers and thus use different ports. Avoid port conflicts. To implement clustering, you run an ant script that makes several related configuration changes *automatically*.

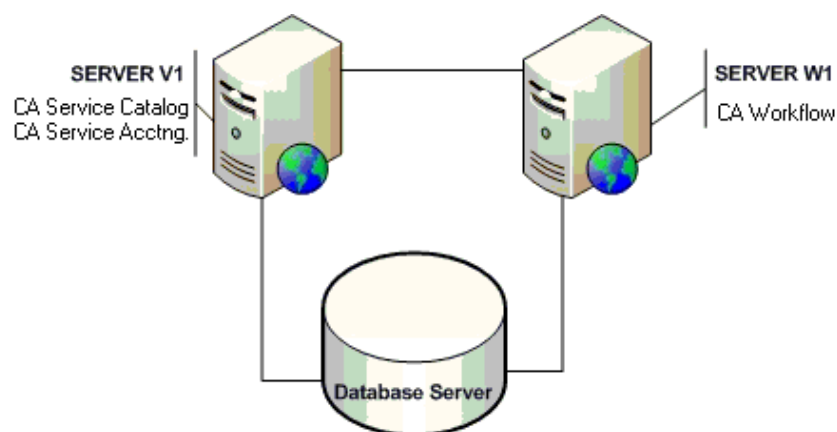
A single application server implemented by a single Java virtual machine (JVM) process cannot always maximize the power and RAM of a large multiprocessor computer. Vertical clustering provides a straightforward mechanism to create multiple JVM processes that together can maximize all the processing power and memory available. Vertical clustering applies to Service View only.

Note: If you are using CA Process Automation as your process automation tool, see your CA Process Automation documentation for information about using clustering with CA Process Automation.

Small Architecture

The small architecture is relatively simple, using three servers. This model is ideal for systems with a load of 1 to 5 catalog requests per minute.

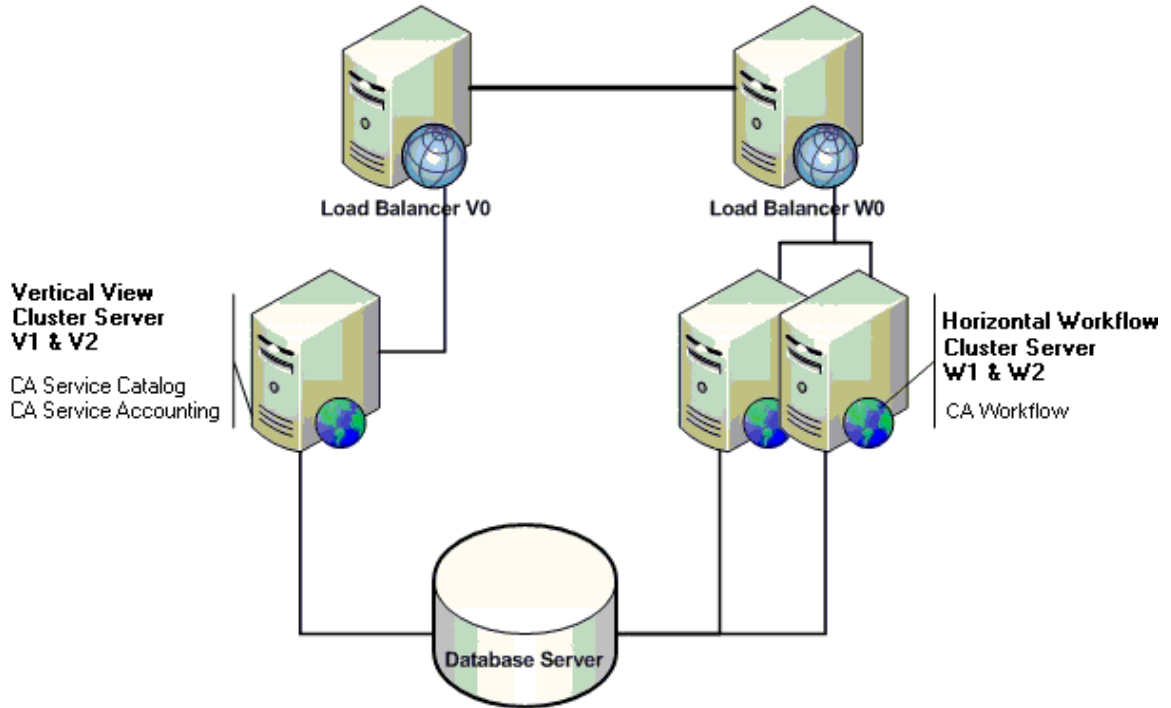
The first server, Server V1, is used to host CA Service Catalog and CA Service Accounting. CA Process Automation or CA Workflow resides on the second server, Server W1. The third server is used to host the DBMS. You can install CA EEM on the database server, if it not installed on another computer in the network.



Medium Architecture

The medium architecture employs vertical [clustering](#) (see page 14) for CA Service Catalog and CA Service Accounting and horizontal clustering for CA Workflow.

The medium architecture can efficiently process a load of up to 10 catalog requests per minute. Both the CA Service Catalog and CA Workflow clusters require a load balancer (Server W0), which can be an existing instance.



Two servers, V1 and V2, exist in a vertical cluster, and reside on the same physical computer. Both V1 and V2 run CA Service Catalog and CA Service Accounting.

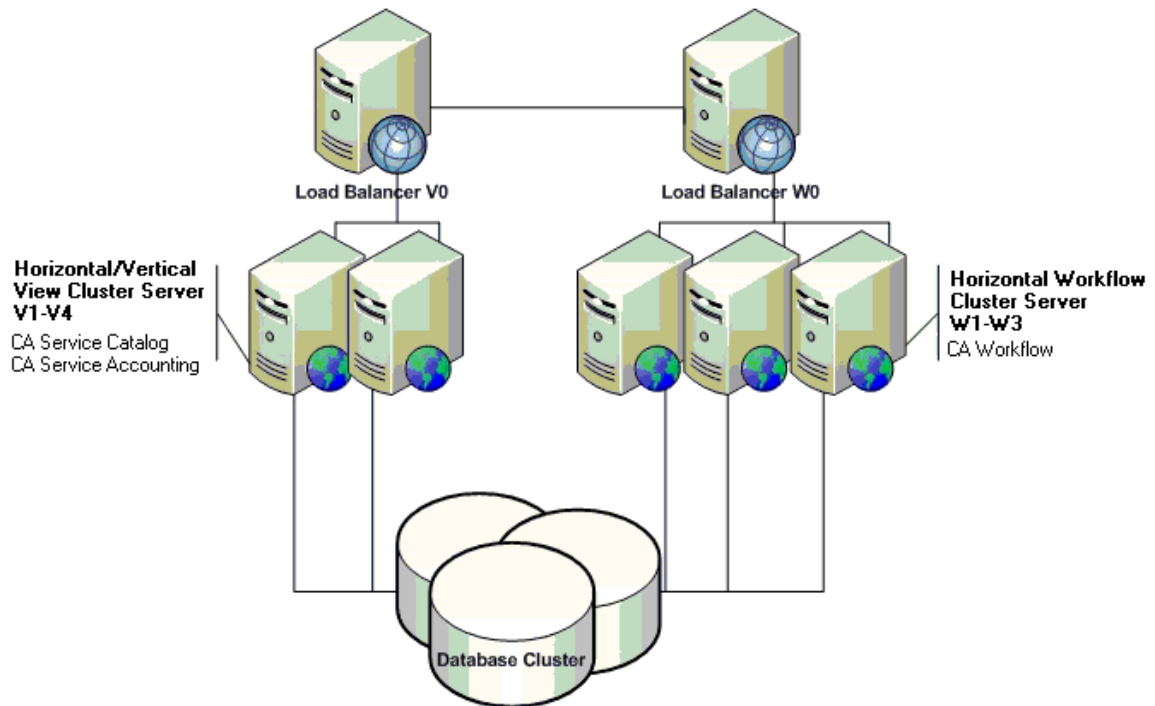
You install and cluster CA Process Automation according to the specifications in the CA Process Automation documentation. Alternatively, you install CA Workflow in a horizontal cluster on two servers, W1 and W2.

Two load balancers, V0 and W0, are the front ends to the Service View clusters and CA Process Automation clusters (or CA Workflow clusters), respectively.

Note: V0 and W0 can be the same computer.

Large Architecture

The large architecture includes clustered multiple web server [clusters](#) (see page 14) and a database cluster, as follows:



You install CA Service Catalog and CA Service Accounting on two physical computers, each one having two horizontal or vertical clusters. Thus, there are four servers named V1 through V4. Alternatively, you could configure these servers as a single horizontal or vertical cluster instead.

You install and cluster CA Process Automation according to the specifications in the CA Process Automation documentation. Alternatively, you install CA Workflow on three physical computers and place them in a separate, vertical cluster.

You replace the database server with a cluster to improve throughput and responsiveness.

Failover Mechanisms

As part of your implementation, you can perform the following tasks to provide failover mechanisms:

- Deploy CA Service Catalog in either a horizontal or vertical cluster, provided through Service View [clustering](#) (see page 14).
- If you use CA Workflow, Deploy CA Workflow in a horizontal cluster.
- If you use CA Process Automation, deploy clustering in CA Process Automation.
- Use *database* clusters. CA Service Catalog components are also compatible with database clusters which are recommended for environments experiencing heavy load.

Note: For information about database clustering, see your DBMS documentation.

- Use a load balancer. Clustering requires a load balancer. To maximize the uptime of CA Service Catalog, include the load balancer and cluster computers in your failover plan.
- Implement clustering on the load balancer computer.
- Move user-generated files from the local file system to a [filestore](#) (see page 187) (a central location) on a high-availability network shared file system. Catalog maintains several user-generated files on the local file system. These files include forms and XSL and XML customizations.
- If you are using CA EEM for authentication, cluster CA EEM, using operating system level clustering.

Note: For information about clustering and implementing failover with CA EEM, see your CA EEM documentation.

- Improve the robustness of the hardware used in your environment, by using all applicable means, including RAID hard disks, redundant power supply, and network cards.

Note: For information about using these means, see your hardware documentation.

Session Management

Session management is very important for performance. One key factor is managing your sessions efficiently is ensuring that you are using CA Process Automation or CA Workflow efficiently, because these tools create and manage sessions.

Effective use of web service sessions is crucial for maintaining throughput as your environment scales up. Creating a web service session is a non-trivial task which requires multiple invocations of authentication and authorization logic and accounts of the majority of time and effort spent when using web services. Design CA Process Automation processes or CA Workflow process definitions and other web service clients to avoid creating extra web service sessions. Exception handling should create a session *only* when the exception is known to be the result of an invalid or expired session.

Note: For details about using CA Process Automation or CA Workflow, see the *Integration Guide*.

Scenario

This topic explains how to architect the CA Service Catalog system to meet the requirements for the following scenario: "I have 60,000 end users distributed across the country and my system is located in a centralized data center owned by the service provider. We may also need to integrate with CA Service Desk Manager, CA APM, and other products. Our expected load is about 100 requests per day with an average of 1000 concurrent connections. We are planning to define CA Workflow processes to meet our requirements."

This scenario is common. Because of the variability around usage patterns and architecture there is no simple calculator that can generate sizing estimates. However, the CA Service Catalog components are dynamically scalable.

The CA Service Catalog architecture is n-tier, stateless, and web-based. Users make HTTP requests. These HTTP requests are passed to one or more application servers and the application server performs the processing logic using a pool of connections to the database. The web server can be co-located with application server instances. In addition, several computational engines run independently from any user interactions; examples include the billing, SLA correlation, and CA Workflow engines. Several additional web servers, application servers, and computational engines can be added, as needed. The database, where state is maintained, is the potential performance bottleneck. The scalability of the database platform is very important. Therefore, the sizing and architecture of the MDB is the most critical factor.

Metrics

First, consider the concurrent connection metric: Because HTTP is connectionless, there is no "concurrent user" metric.

Next, consider the metric of 100 requests per day: This metric does not provide the peak usage, a critical factor. If the 100 requests are evenly distributed through the day, system impact would be minimal. However if the 100 requests are all made at the same time of day, then the system could potentially be challenged. Also, the type of request has a direct impact on the resource utilization.

Variations

Variations in usage and architecture are important. Consider them carefully and tune your system accordingly to account for them. You may need to adjust your tuning over time as changes in demand or system load occur.

Business Requirements and Updates

When you are implementing CA Service Catalog, it is critical to capture accurate business requirements and use them to formulate efficient technical architectures. Therefore, you start an implementation with a discovery phase per module to capture the business requirements (functional and non-functional). Next, you study the limitations and capabilities of the client operational infrastructure, and you formulate an efficient implementation architecture. With all the information you have obtained, you can formulate an initial sizing estimate.

Based on the many types of possible variations in usage and architecture, organizations should start with two instances of each component for fail-over and load balancing. Because components can be co-located, start with at least two server class machines in addition to the database server or servers. If computational engines (for example, from billing or CA Workflow) are heavily used during peak activity times, they may require their own server or servers. Clients' usage-patterns typically change over time as they grow to understand a product's features and use them more heavily. As you discover usage patterns over time, you can dynamically add and distribute components as needed.

Clustering

As a CA Service Catalog administrator, you can optionally use *clustering* for CA Workflow and Service View to improve performance and provide *failover protection*. Here, the term *clustering* means multiple computers grouped together performing the same or similar function, essentially acting as one virtual computer. Specifically, clustering here refers to CA Workflow and Service View running on two or more computers. *Failover protection* means that if one computer malfunctions, becomes heavily loaded, or loses power, its workload is transferred to the other computers in the cluster. These computers retain and complete the active sessions.

Another advantage of clustering is *load-balancing*: If one of the cluster components is busy processing a request, the load is redirected to another component in the cluster. Users of the system see no interruption of access. CA Workflow and Service View processing for CA Service Catalog continues. The loss of performance on users and business functions is minimized, even when computer availability is lost or reduced.

As a CA Service Catalog administrator, you can [implement clustering](#) (see page 215) for Service View, CA Workflow, or both.

Note: If you are using CA Process Automation, you can also implement clustering for CA Process Automation. The CA Process Automation documentation and installation media are included with the CA Service Catalog installation media.

Authentication Methods

Administrators can authenticate users in CA Service Catalog with the following means:

- CA EEM alone
- CA EEM with an external directory; for example: an LDAP directory, such as Microsoft Active Directory

Note: For instructions to configure CA EEM, with or without an external directory, see the *Integration Guide*.

- [Windows NTLM authentication](#) (see page 105)

Products and Components Overview

The installation media includes the following CA Service Catalog products and related components:

CA Service Catalog, CA Service Accounting, and Service View

CA Service Catalog provides a container that consists of services published by a business unit or throughout the enterprise. Services are built of one or more service option groups that describe IT services and how to charge for them.

The service catalog also enables an organization to model its business units or departments and manage the users accounts contained within those units. Services in the service catalog may be organized into folders and may contain detailed information about the price of a service. Services may represent one or more metrics and may include Service Level Agreements (SLAs).

CA Service Accounting is a financial component of CA Service Catalog that allows IT departments or other organizations to perform billing, chargeback, cost allocation, budgeting and planning of IT Services or anything else that is published in the catalog.

CA Service Catalog includes a component named Service View, its web-based user interface. Service View handles the processing of requests for service by each product and component.

CA Service Catalog also provides required common functions such as management of users, business units and accounts, reporting, event handling, and so on.

Catalog Content

The installation media includes the Catalog Content, a set of many best practice model services to help you start your catalog quickly and efficiently. Using these model services helps you better align your services with business goals, improve internal customer satisfaction, and standardize your processes to achieve greater operational efficiency.

CA MDB, CA EEM, and CA Workflow

CA MDB, CA EEM, and CA Workflow are integrating products supplied on the CA Service Catalog installation media.

Overview of Integrations

The products that integrate with CA Service Catalog can be grouped according to those that are supplied and licensed with CA Service Catalog and those that are supplied and licensed separately.

Integrations Supplied on the CA Service Catalog Installation Media

The following integrating products and components are included when you purchase CA Service Catalog and are licensed with it. These products are supplied on the CA Service Catalog installation media. You install these products and components individually as part of the CA Service Catalog installation process.

CA Management Database (CA MDB)

Many CA products, including CA Service Catalog, share a common, required database schema named the CA Management Database (CA MDB or the MDB).

During the installation or upgrade of Service View, the MDB is automatically created or updated (if necessary) and is configured in the database management system (DBMS).

Note: You must install SQL Server or Oracle before installing CA Service Catalog. For more information on supported versions of the DBMS, see the *Release Notes*.

We recommend that CA Service Catalog and all CA products that integrate with it share the same CA Management Database (CA MDB). CA Service Catalog embeds CA MDB r1.5. To integrate CA Service Catalog with other CA products that embed CA MDB r1.5 or CA MDB r1.0.4, [verify the CA MDB version compatibility for your integrations](#) (see page 33).

CA Embedded Entitlements Manager (CA EEM)

CA Service Catalog uses CA EEM to manage authentication and some aspects of authorization. You can optionally use CA SiteMinder instead of CA EEM for authentication.

CA Workflow

CA Workflow automates business processes. CA Service Catalog uses either CA Workflow or CA Process Automation to automate approval and fulfillment process for items requested from the catalog.

Note: For best results, including more efficient process automation, install and use CA Process Automation rather than CA Workflow. For details about installing and using CA Process Automation, see the CA Process Automation installation media, which is included with the CA Service Catalog installation media.

For instructions to install these components, see the *Implementation Guide*. For instructions to set up and use the *integration* between these components and CA Service Catalog, see the *Integration Guide*.

Integrations Supplied in Addition to the CA Service Catalog Installation Media

The following integrating products are included when you purchase CA Service Catalog and are licensed with it. These products are supplied on their own installation media, in addition to the CA Service Catalog installation media. You install these products individually, *either* before or after you install CA Service Catalog.

CA Process Automation

CA Process Automation uses graphical processes created by system administrators to execute operational processes automatically. It supports a fully integrated development and administrative environment to manage, create, and configure CA Process Automation components on your system. CA Process Automation also supports client applications that enable operators and other personnel to schedule, start, and monitor automated processes..

BusinessObjects Enterprise

CA products leverage the most extensive set of business intelligence capabilities, ranging from reporting, query and analysis, by using BusinessObjects Enterprise. BusinessObjects Enterprise is a flexible, scalable, and reliable business intelligence reporting system that can be tightly integrated into your information technology infrastructure.

For instructions to install and configure these components, see their documentation sets. For instructions to set up and use the *integration* between these components and CA Service Catalog, see the *Integration Guide*.

For further information about these components, see their documentation sets. The CA Process Automation documentation set is included on the CA Process Automation installation media, and the BusinessObjects Enterprise documentation is included on the BusinessObjects Enterprise installation media.

Integrations Supplied Separately

The following integrating products are supplied and licensed separately from CA Service Catalog. They are purchased separately from CA Service Catalog and are supplied on their own installation media. All of these integrations are optional. Unless noted otherwise, you install these products individually, before or after you install CA Service Catalog.

CA Service Desk Manager, which includes CA CMDB

CA Service Catalog integrates with CA Service Desk Manager in several ways. CA Service Catalog can automatically open CA Service Desk Manager tickets and attach associated configuration items (assets) using CA Workflow. CA Service Catalog events can also cause a CA Service Desk Manager ticket to be created automatically.

CA Service Catalog can integrate with CA CMDB by associating catalog services with CA CMDB configuration items.

Note: For best results, it is strongly recommended that CA Service Desk Manager and CA Service Catalog share the same CA MDB and the same installation of CA EEM.

CA Business Service Insight

CA Business Service Insight 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 Business Service Insight enables organizations to understand the performance and cost implications of these agreements in real time.

Reservation Manager

Reservation Manager is a separate utility with its own user interface that integrates with CA Server Automation to provide on-demand resources to users for reserving Windows, Linux, AIX, and Solaris systems. You can use Reservation Manager to reserve physical and virtual systems from a pool of available resources in your data center.

CA Asset Portfolio Manager (CA APM)

CA Service Catalog can integrate with CA APM by connecting catalog entries with CA APM Models and connecting requested items with CA APM assets.

Note: To integrate successfully, CA APM and CA Service Catalog must share the same CA MDB.

CA SiteMinder

CA SiteMinder provides web-based single signon and enhanced authentication of CA Service Catalog users.

CA Storage Resource Manager (CA SRM)

Through the integration between CA Service Accounting and CA Storage Resource Manager (CA SRM), usage data that indicates storage used by a user can be invoiced to users' accounts.

CA MICS and CA JARS

Using data from CA Mainframe Information Control System Resource Management (CA MICS) or JARS to supply usage data to CA Service Accounting, accounts can be invoiced for using services recorded by CA MICS or JARS.

For instructions to install, set up, and use these products, see their documentation. For information about which versions of these products integrate with CA Service Catalog, see the *Release Notes*. For instructions to set up and use the *integration* between these components and CA Service Catalog, see the *Integration Guide*.

Chapter 2: Preparing to Install or Upgrade

This section contains the following topics:

[New Installation, Upgrade, or Migration](#) (see page 27)

[Considerations and Requirements Before Installation](#) (see page 28)

New Installation, Upgrade, or Migration

You install, upgrade, or migrate CA Service Catalog as follows:

- If you are installing CA Service Catalog *for the first time*, first you review the [before you install](#) (see page 28) topics and next you [install](#) (see page 40) CA Service Catalog.
- If you are upgrading CA Service Catalog from a previous release, do the following:
 - Review the [scope and limitations of an upgrade](#) (see page 56)
 - Upgrade using either a traditional model or a migration model.
- If you are moving the same release of CA Service Catalog, for example, from test to production, or as part of a disaster recovery process, you perform a [migration](#) (see page 73).

Considerations and Requirements Before Installation

Addressing the following considerations and requirements before installation helps you install the product correctly and also helps the product to run efficiently.

Where applicable, find and record installation-related data and have it ready when you begin the installation.

The considerations and requirements follow:

- [Release Notes](#) (see page 28)
- [System requirements and related requirements](#) (see page 29)
- [Authentication and authorization](#) (see page 35)
- [DBMS and CA MDB](#) (see page 32)
- [Operating system](#) (see page 29) and [operating system language](#) (see page 29)
- [Host names and port numbers](#) (see page 35)
- [Server architecture](#) (see page 36)
- [Web application servers](#) (see page 29)
- [Service Provider business unit](#) (see page 37)

Release Notes

You can find the *Release Notes* and *Readme* (if supplied) on the installation media.

The *Release Notes* contains the [system requirements and related requirements](#) (see page 29). The computers on which you install or upgrade CA Service Catalog components must meet or exceed these requirements. The *Release Notes* also contains any important installation-related information that became known after the *Implementation Guide* was finalized. Finally, the *Release Notes* also provides general information about the documentation set, integrating products, localization, and known issues.

A readme file is optional and is included *only* if necessary to explain last-minute information that became known after the other documentation was published.

For the most recent documentation, including the *Release Notes*, see Technical Support at <http://ca.com/support>.

Operating System

You can install CA Service Catalog products and components on supported Windows Server operating systems only!

Note: For more information about system requirements for CA Service Catalog, see the *Release Notes*.

Operating System Language

CA Service Catalog is certified on several operating system languages. Language certification means that you can install and run the product correctly for the supported operating systems in the supported language. Likewise, the product can store and retrieve data using the character set of the supported language.

Note: Verify that all server operating systems use the same language. For the list of supported languages, see the *Release Notes*.

Web Application Servers

You can select your web application servers from the list of supported application servers.

More information: For details about supported application servers, see the *Release Notes*.

System Requirements and Related Requirements

To run efficiently, CA Service Catalog components must be installed on computers that meet certain hardware and software requirements. For details about these requirements, see the *Release Notes*.

Related requirements include the following:

- [General considerations and requirements](#) (see page 30)
- [Distributed considerations and requirements](#) (see page 31)
- [Network share considerations and requirements](#) (see page 31)

General Considerations and Requirements

Review this section for important information regarding new installations and upgrades.

The following installation considerations and requirements typically apply to all implementations.

- Service View must be installed first, before any other CA Service Catalog product or component is installed.
- Verify that all CA Service Catalog computers are *geographically colocated*—that is, are located in the same building, in the same room. Having all CA Service Catalog computers geographically colocated helps prevent possible performance problems that network latency could cause.

The term *CA Service Catalog computer* means the DBMS server and any computer on which you plan to install any CA Service Catalog product or component. These products and components include CA EEM, CA Workflow, and other CA Technologies products or components included on the CA Service Catalog installation media.

- Verify that the computer on which you plan to install any CA Service Catalog component or the MDB meets the applicable system requirements.
- Before you upgrade, note the value of all Use Service Provider Catalog Option settings for all business units in your implementation. Decide which one to use as a system setting in CA Service Catalog. After you upgrade, set this parameter to match your decision.
- Back up your entire system before upgrading from a previous release of CA Service Catalog to this release. Similarly, after you have installed this release, back up your entire system before migrating from test to production.
- In this release, you use a single new administration configuration option to enable [Windows NTLM authentication](#) (see page 105). This option is named Single Signon Authentication. This option simplifies your configuration process by replacing the manual editing of XML files used in previous releases.
- Log in to CA Service Catalog computers using the Administrator account.
- We recommend that you do not add users, delete users, or change user information using CA EEM. Instead, use CA Service Catalog, which integrate with CA EEM and update CA EEM accordingly.
- If you are installing on a Windows 2008 computer with Terminal Server, close the installation dialog after you install each CA Service Catalog product and component. Otherwise, the next attempt to install a CA Service Catalog product and component could fail.

- The Application User is automatically created during the installation.
The CA Service Catalog product user named *spadmin* is automatically created as a product user. The password for this user is also *spadmin*.
- After you have installed Service View, restart the computer on which you installed it.
- After you complete an upgrade, verify that the events, rules, and actions that you had enabled before the upgrade are still enabled.

Distributed Considerations and Requirements

When you install CA Service Catalog products and components on multiple computers (a distributed implementation), meet the following requirements:

- The first CA Service Catalog product or component that you install on any computer must be Service View.
- You can install CA Service Accounting and CA Workflow on different computers than Service View. However, you install CA Service Catalog and Catalog Content on the *first* (formerly *primary*) Service View computer *only*.
- Any computer on which you install Service View, CA Service Catalog, Catalog Content, CA Workflow, or CA Service Accounting must have either your DBMS server or DBMS client installed. This requirement applies to both SQL Server and Oracle.

Important! If you use CA Process Automation, we recommend that you do *not* install the CA Process Automation domain orchestrator and CA Process Automation components on the same computer.

Network Share Considerations and Requirements

When you install CA Service Catalog products and components on a network share, follow these considerations and requirements:

- If the installation image is on a network share, then map a drive letter to this share. You *cannot* run batch files from a UNC path.
- We recommend that you copy the installation image to a local folder and run the installation programs locally.

Requirements and Considerations for the DBMS and CA MDB

These requirements and considerations are as follows:

- [Database management system](#) (see page 32)
- [CA MDB character set for localization support](#) (see page 32)
- [MDB version compatibility for integrations](#) (see page 33)
- [CA MDB documentation](#) (see page 34)
- [Case sensitivity](#) (see page 34)

Database Management System

CA Service Catalog supports the following database management systems:

- Microsoft SQL Server 2005 or 2008 running on Windows
- Oracle 10g R2 or 11g R2 running on Windows or Linux

If you are implementing CA Service Catalog in a multilingual environment, verify that your DBMS supports Unicode for double-byte languages. For example, if you are using Oracle, install Oracle with Unicode Support to help ensure that localized double-byte characters display correctly.

Important! If you are using a version of Oracle or SQL Server that CA Service Catalog does not support, do the following: Back up your database, upgrade to a supported version of DBMS software, and install CA Service Catalog.

Note: For details about supported versions of database management systems, see the *Release Notes*.

CA MDB Character Set for Localization Support

Because the CA Management Database (CA MDB) is shared, all CA products sharing the same CA MDB must use the same language. Otherwise, shared information could be expressed improperly. Follow these guidelines for collations in SQL Server and character sets in Oracle:

- Collations in SQL Server

CA MDB honors the default setting of the SQL Server instance collation as case insensitive. CA Service Catalog honors the setting of the CA MDB collation and inserts the default data into the database, if the local operating system supports the data set.

If the local operating system does *not* support the data set, then it inserts the default data as English. For example, if CA Service Catalog is deployed in a French operating system, then the default data set is inserted in French. No special configuration is required for international character support.

- Character sets in Oracle

While you are installing Oracle server, do the following:

- To configure CA MDB to support only the language of the operating system, select the default character setting.
- To configure CA MDB to support multiple languages, select Unicode (AL32UTF8).

Note: For more information about the MDB, see the *CA MDB Overview*. For details about the list of languages supported for localization, see the *Release Notes*.

How to Verify CA MDB Version Compatibility for Integrations

CA Service Catalog embeds CA Management Database (CA MDB) r1.5. CA Service Catalog integrates with other CA products that embed either CA MDB r1.5 or r1.0.4. For best results, verify that CA Service Catalog and all integrated CA products share the same CA MDB, as follows:

Review the following scenarios for integrating with other CA products that run either CA MDB r1.5 or CA MDB r1.0.4. Determine the scenario that matches your environment and follow the accompanying instructions.

- You want to integrate CA Service Catalog with *only* other CA Technologies products that also embed CA MDB r1.5, such as the current release of CA Service Desk Manager.

Install CA Service Catalog and these other products. The same CA MDB r1.5 database is automatically shared among all these CA Technologies products and runs in single-version MDB mode.

- You want to integrate CA Service Catalog with CA Technologies products that embed CA MDB r1.0.4. You have already installed at least one of them, but you have not yet installed CA Service Catalog. The CA MDB r1.0.4 products include CA CMDB r11.2, Unicenter Service Desk r11.2, and CA APM r11.3.

When you install CA Service Catalog, the embedded CA MDB r1.5 installer automatically upgrades CA MDB r1.0.4 to CA MDB r1.5. The database is automatically shared among all these CA Technologies products and runs in mixed-version MDB mode.

- You want to integrate CA Service Catalog with CA MDB r1.0.4 products. You have already installed CA Service Catalog, and you plan to install one or more CA MDB r1.0.4 products later.

Do the following:

1. Apply the CA MDB r1.0.4 Compatibility Patch to enable the integration between both versions of the CA MDB.

Note: For details about installing this patch, see the *Integration Guide*.

2. Install any of these CA Technologies products that you have not yet installed.

The database is shared among all these CA Technologies products and runs in mixed-version CA MDB mode.

Note: The CA Service Catalog installation media includes the *CA MDB Overview Guide*. Other CA MDB documentation is available from CA Technical Support at <http://supportconnect.ca.com>.

CA MDB Documentation

Verify that the system on which you are installing the database management system software meets the MDB requirements stated in the MDB documentation.

If necessary, the MDB installation or upgrade starts automatically when you attempt to install or upgrade the first (formerly *primary*) Service View computer. During this MDB installation or upgrade, you supply required parameter values, such as the server name, logon credentials, and port numbers, for your DBMS.

The *CA MDB Overview Guide* is included with the CA Service Catalog documentation, on the CA Service Catalog bookshelf. As a best practice, review this document before installing CA Service Catalog.

Case Sensitivity

CA Service Catalog and CA Service Accounting inherit CA MDB case-sensitivity characteristics. If SQL Server is the DBMS for CA MDB, then searches in CA Service Catalog and CA Service Accounting are case insensitive by default. Therefore, by default, you see case-sensitive search results for a field only if the field is defined explicitly as case sensitive.

Similarly, if Oracle is the DBMS for CA MDB, then searches in CA Service Catalog and CA Service Accounting use the Oracle DBMS characteristics. In that case, you expect case-sensitive searches.

For example, suppose you search for an account by clicking Home, Search, Account. With SQL Server, you expect case-insensitive search results. In contrast, with Oracle, you expect case-sensitive search results.

Authentication and Authorization

You can use CA EEM to *authenticate* and *authorize* users. *Authentication* means using a user ID and password or other means to verify that the user is a valid user of the system. *Authorization* means validating that the logged in user can access particular functionality in the product.

You specify whether to use CA EEM standalone or with an external directory. When you use CA EEM standalone, CA EEM stores the user information and passwords in its data store. When you use CA EEM with an external directory, such as Microsoft Active Directory, the external directory stores the users and passwords in its data store.

- To install any CA Service Catalog component, log on to your computer as an Administrator. Verify that you have local administrator privileges on the servers that you plan to use.
- If you are using an existing CA EEM instance, have the server name and password for the EiamAdmin user available.
- CA Service Catalog can send emails in certain situations. Have your email server name available.

In addition, if the client system uses a Windows domain, you can configure CA Service Catalog to use [NTLM authentication](#) (see page 105). NTLM authentication enables a user who has been authenticated to the domain to skip the login page.

Host Names and Port Numbers

During the installation, you specify the host names of the computers on which to install CA Service Catalog components.

On each CA Service Catalog computer, you also specify the port number to use for communicating with other CA products, such as CA Business Service Insight, CA Service Desk Manager, or CA APM.

The following port numbers are the default values for CA Service Catalog. You can change them during installation. If these ports are not available, have other nonconflicting port numbers available.

- 8080 and 8085 – For the Service View service for HTTP communication
- 8443 – For the Service View service for HTTPS communication

The following port numbers are the default values for CA Workflow. You can change them during installation. If these ports are not available, have other nonconflicting port numbers available.

- 8090 and 8095 – For the CA Service Fulfillment service (CA Workflow) for HTTP communication
- 8444 – For the CA Service Fulfillment service (CA Workflow) for HTTPS communication

The following port number is the default values for use by CA EEM. You cannot change it during installation.

- 5250 – Used by the iTechnology iGateway service

Server Architecture

The CA Service Catalog architecture allows components to be distributed on multiple servers. All product components can be installed on the same server; however, this single server architecture is not optimal for performance. We recommend that you install the database on a server that does not have CA Service Catalog products and components installed. You can install CA EEM on the same server as the database. Follow these guidelines:

- To distribute the processing load, you can optionally install many of the CA Service Catalog components on separate servers.
- Service View is the first CA Service Catalog component that you install. The first Service View server installed is named the *first* (formerly *primary*) Service View server. You can also install Service View on *additional* (formerly *secondary*) Service View servers to distribute the load of processing catalog requests.
- You can install CA Service Accounting on the first Service View server or on other computers. You can optionally install CA Service Accounting multiple times on multiple computers, to distribute the processing load of billing runs automatically.
- You can optionally install CA Workflow multiple times on multiple computers.
Note: CA Service Catalog uses Java Web Start to start the CA Workflow Process Definition Tool (IDE) on your local computer automatically, if applicable.
- To distribute the processing load more evenly, you can do the following:
 - Direct users to separate Service View servers by having them use different URLs to log on to CA Service Catalog
 - Use [clustering](#) (see page 21) for Service View and for CA Workflow (if used) and CA Process Automation (if used)

Service Provider Business Unit ID

During the Service View installation, you specify a “service provider” business unit ID. This ID specifies the top level (root) business unit. All other business units are structured under the root business unit. As a best practice, specify your company domain name or a short version of your company name for this ID.

Decide the “service provider” business unit ID *before* the installation. After you have installed CA Service Catalog, the following conditions exist:

- You *cannot* change the business unit *ID* of the service provider.
- You *can* change the business unit *login ID* and the business unit name service provider.

Chapter 3: Installing

This section contains the following topics:

[How to Install](#) (see page 40)

[CA EEM Installation Considerations](#) (see page 41)

[Install CA EEM](#) (see page 41)

[How to Prepare for the MDB Installation or Upgrade](#) (see page 42)

[Install Service View](#) (see page 46)

[Install CA Service Catalog](#) (see page 48)

[Installation of a Process Automation Tool](#) (see page 49)

[Install CA Workflow](#) (see page 49)

[Install Catalog Content](#) (see page 51)

[Install CA Service Accounting](#) (see page 52)

[Installation and Configuration Procedures for Third-Party Unicode Fonts](#) (see page 53)

How to Install

Important! If you have copied the installation media to a network share, map a drive letter to this share. This mapping is required because a BAT file runs as part of the installation, and BAT files cannot run from a UNC path.

CA Service Catalog includes several products and components. To install them, follow this process:

1. Verify that you have followed the [considerations and requirements](#) (see page 28) that apply before installation. Especially verify that all CA Service Catalog computers are *geographically colocated*, that is, are located in the same building, in the same room.
2. Install your DBMS, if it is not already installed.
3. Install Java Runtime Environment (JRE) from the CA Service Catalog installation media.
4. [Install CA EEM](#) (see page 41).
5. [Prepare for the MDB installation or upgrade](#) (see page 42).
6. [Install the first Service View computer](#) (see page 46); the installation program installs or upgrades the MDB as part of this procedure.

Important! We recommend that CA Service Catalog and all CA products that integrate with it share the same CA Management Database (CA MDB). CA Service Catalog embeds CA MDB r1.5. To integrate CA Service Catalog with other CA products that embed CA MDB r1.5 or CA MDB r1.0.4, [verify the CA MDB version compatibility for your integrations](#) (see page 33).

7. Install *additional* (formerly *secondary*) Service View computer, if applicable.
8. [Install CA Service Catalog](#) (see page 48).
9. [Install CA Process Automation \(the recommended process automation tool\) or CA Workflow](#) (see page 49).
10. [Install Catalog Content](#) (see page 51).
11. [Install CA Service Accounting](#) (see page 52). Optionally install additional instances of CA Service Accounting.
12. [Install and configure third-party unicode fonts](#) (see page 53). This task is required *only* if you want to enable Report Data Views to support double-byte characters in PDF export.

The installation is completed.

For better performance, consider implementing [clustering](#) (see page 21) for Service View, CA Workflow, or both.

CA EEM Installation Considerations

Consider the following *before* you [install CA EEM](#) (see page 41):

- You can optionally install CA EEM on the *same* server as the *first* (formerly *primary*) Service View server.
- For best performance, install CA EEM on a different server than the DBMS server.
- If you are installing CA EEM on a 64-bit computer that has CA Anti-Virus or CA Threat Manager installed, do the following: Uninstall that software before installing CA EEM and reinstall that software after installing CA EEM.

Important! CA Service Catalog requires CA EEM r8.4 SP4. For the latest certification information for CA Service Catalog, CA Service Accounting, CA EEM, and related CA products and components, see the Certification Matrix for each of them on <http://ca.com/support>.

Install CA EEM

Installing CA EEM is a required task when you [install CA Service Catalog products and components](#) (see page 40). CA EEM authenticates users during login and authorizes users to access CA Service Catalog.

Follow these steps:

1. Review the [installation considerations](#) (see page 41).
2. If you have not already installed Java Runtime Environment (JRE) 1.6 (or higher) and you plan to integrate CA EEM with CA SiteMinder, perform this step to install JRE. Otherwise, skip this step:
 - a. Locate the file named jre-windows-i586 in the Utilities\Java folder.
 - b. Double-click the file to install it.
 - c. Follow the prompts to complete the installation.
 - d. Record the complete path name of the installation for use in a later step.
3. Start the setup.exe file on the CA Service Catalog installation media.
The Product Explorer window of the installation program appears.
4. Select Utilities, CA EEM, and click Install.
The installation wizard guides you through the installation process.
5. Enter the value of the EiamAdmin password that you want to use, when prompted.
Record this password for future reference.

6. When you are prompted for the Java Home directory, leave the value empty and click Skip, unless you plan to do one or both of the following:

- Integrate CA EEM with CA SiteMinder
- Use Security Assertions Markup Language (SAML) with CA EEM

If you plan to perform either of these tasks, enter the complete path name of your Java Runtime Environment (JRE) installation.

7. Continue following the wizard instructions and complete the CA EEM installation.
8. Reinstall CA Anti-Virus or CA Threat Manager, if you uninstalled it earlier.

You have installed CA EEM.

Note: For instructions to configure and use CA EEM, see the *Integration Guide*.

How to Prepare for the MDB Installation or Upgrade

Preparing for the MDB installation or upgrade is a required task when you [install CA Service Catalog products and components](#) (see page 40). The MDB is the common, shared database for your CA products. The MDB provides the database schema required by CA Service Catalog and other CA products. During the CA Service Catalog installation, the MDB is installed or upgraded automatically, if necessary. For CA Service Catalog, perform the following tasks to prepare for the MDB installation or upgrade. These tasks apply to all DBMS.

1. Review the Management Database documentation, which is supplied with other documents on the CA Service Catalog installation media. Note the most applicable information for your implementation plans, and keep it on hand for reference.
2. Apply all SQL Server or Oracle patches and other maintenance.
For details, see your SQL Server or Oracle documentation.
3. Verify that SQL Server or Oracle is installed and running.
4. Decide whether to install the *first* Service View server on the *same* computer as your SQL Server server or Oracle server or on a *different* computer. The first Service View server is the first CA Service Catalog component that you install. Decide as follows:
 - For best performance, install the SQL Server server or Oracle server and the first Service View server on *different* computers—we recommend this option.
 - If the server has enough resources, optionally install the first Service View server on the same computer as the SQL Server server or Oracle server.

Before you finalize your choice, review the MDB documentation for any applicable concerns.

5. Install your DBMS client on each required computer, as follows: The SQL Server client is required on any computer (except the SQL Server server) on which a CA Service Catalog component is installed. Likewise, the Oracle client is required on any computer (except the Oracle server) on which a CA Service Catalog component is installed.

In both cases, the client enables CA Service Catalog components to communicate with the database. For details, see your SQL Server or Oracle documentation.

6. Find and record the values for the MDB parameters, *one* of the following:

- [Parameters for MDB on SQL Server](#) (see page 43)
- [Parameters for MDB on Oracle](#) (see page 44)

Have these values ready when you begin to [install the first Service View computer](#) (see page 46).

When you begin that installation or upgrade, the MDB installation or upgrade starts automatically, if necessary, and you are prompted to supply these values.

7. Remove replication in your DBMS.

Important! When replication has been added, the database tables are locked from any schema changes, even if replication is turned off. As a result, the upgrade cannot run successfully.

Note: For instructions to remove replication, see your DBMS documentation. Also see that documentation for instructions to add it again, after you have completed the upgrade.

You have prepared for the MDB installation or upgrade.

Parameters for MDB on SQL Server

If the MDB installation or upgrade starts automatically when you begin to [install the first Service View computer](#) (see page 46), you supply values for the following parameters. Therefore, before starting to install or upgrade the first Service View, record these values, and have them ready. The exact parameters that appear depend on whether you are performing a new installation or an upgrade.

Host Name

Defines the computer name of the Microsoft SQL Server (SQL Server) server and the instance name, if used. The default is the host name of the local host.

If you are using instances, append the instance name to the computer name; otherwise, specify only the computer name.

DBMS Instance Name

Defines the SQL Server instance name for the MDB. For example, myinstance.
The default value is mssqlserver.

Important! Instances must reside on a static port!

Listen Port

Defines the TCP Port number. The default is 1433.

MDB Administrator Password

Defines the password for the MDB Administrator (for upgrades only).

User Name

Defines the name of the SQL Server database administrator (DBA) user. The default is sa.

Password

Defines the password of the SQL Server database administrator (DBA) user.

usmuser

Defines the user ID that CA Service Catalog uses to access the database. The default value is usmuser.

usmuser Password

Defines the password for usmuser.

Parameters for MDB on Oracle

If the MDB installation or upgrade starts automatically when you begin to [install the first Service View computer](#) (see page 46), you supply values for the following parameters. Therefore, before starting to install or upgrade the first Service View, record these values, and have them ready. The exact parameters that appear depend on whether you are performing a new installation or an upgrade.

Note: These parameters apply to Oracle running on both Windows and Linux.

Host Name

Defines the computer name of the Oracle server. The default is the host name of the local host, for example, ServDeliv12.

Service Name

Defines the service name. Every Oracle database or service has a service name. The service name of an Oracle database is typically its global database name. Enter the service name of the Oracle database or other service that you want to access.

Important! The service name *cannot* be longer than eight characters.

Connection ID

Defines the connection ID (such as orcl) for connecting to the Oracle server, as follows:

- For a local database, this value is typically the SID.
- For a remote database, this value is typically the Net Service Name.

Listen Port

Defines the TCP Port number. The default is 1521.

Tablespace Path

Defines the complete path name of the tablespace for Oracle.

MDB Administrator Password

Defines the password for the MDB Administrator. Applies to upgrades only.

DBA User Name

Defines the Oracle DBA user. The default is SYS.

DBA Password

Defines the DBA user password.

Data Tablespace Name

Defines the tablespace name for the data.

Index Tablespace Name

Defines the tablespace name for the indexes.

The installer checks whether the data and index tablespaces exist in the MDB. These tablespaces exist when either of the following conditions are met:

- The MDB is being upgraded.
- The MBD is used with another MDB that is installed by any integrated component such as CA Process Automation or CA Service Desk Manager.

If the data and index tablespaces exist, the installer displays their names. The installer also prompts you to specify whether to continue using the existing names or overwrite them with new names.

usmuser

Defines the user ID for the CA Service Catalog products to use for accessing the database. The default value is usmuser.

usmuser Password

Defines the password for the user named usmuser.

Install Service View

When you [install CA Service Catalog products and components](#) (see page 40), installing the first (formerly *primary*) Service View computer is a required task. Afterwards, you can optionally install *additional* (formerly *secondary*) Service View computers. When you begin to install or upgrade the first Service View computer, the MDB installation or upgrade starts automatically, if necessary. If applicable, install or upgrade the MDB when you are prompted to do so.

Important! Install CA EEM *before* you install Service View. Also, verify that the DBMS client (Oracle client or SQL Server client) is installed locally, unless this computer is the DBMS server. For instructions to install the DBMS client, see your DBMS documentation

Follow these steps:

1. Access the root folder on the installation media and run setup.exe.
The installation Product Explorer window appears.
2. Select Service View, Windows and click Install.
The installation wizard guides you through the installation process.
3. Select the option for the *first* Service View server, if applicable. Otherwise, leave this option unselected to install an *additional* (formerly *secondary*) Service View server.
4. Select the database type and click Next.
5. If the MDB installation or upgrade starts, do the following:
 - a. Enter the values that you recorded when you prepared to install or upgrade the MDB (*one* of the following), and click Next.
 - [Parameters for MDB on SQL Server](#) (see page 43)
 - [Parameters for MDB on Oracle](#) (see page 44)
 - b. For log information for SQL Server, see the following:
 - See the install_mdb.log file and the configureMSSQLMDB.log file in your MDB target installation directory. This directory is specified in %TEMP%\MDB1.5, where %TEMP% is Windows environment variable. If the MDB installation fails, review the log files in this location.
 - After a successful installation of the MDB, the install_mdb.log file is copied to the %ProgramFiles%\CA\SC\Mdb\Windows\logs folder. This log file is renamed to install_mdb_mm-dd, hh_mm_ss.log (for example, install_mdb_12-03,15_29_05.log).
 - After a successful installation of both the MDB and Service View, configureMSSQLMDB.log is copied to the %USM_HOME%\logs\install folder.

- c. For log information for Oracle, see the following:
 - See the files named `configureOracleMDB.log` and `install_connectionID.log` in your MDB target installation directory. For example, if the connection ID is `myhost_orcl`, the `install_connectionID.log` file name is `install_myhost_orcl.log`. The MDB target installation directory is specified in `%TEMP%\MDB1.5`, where `%TEMP%` is Windows environment variable. If the MDB installation fails, review the log files in this location.
 - After a successful installation of the MDB, the `install_connectionID.log` file is copied to `%ProgramFiles%\CA\SC\Mdb\Windows\logs`. This log file is renamed to `install_connectionID_mm-dd,hh_mm_ss.log`, for example, `install_myhost_orcl_12-03,15_29_05.log`.
 - After a successful installation of both the MDB and Service View, `configureOracleMDB.log` file is copied to the `%USM_HOME%\logs\install` folder.

6. Do the following when you are prompted to supply the CA EEM server host name and password:
 - a. Confirm or correct the CA EEM server host name.
 - b. For the CA EEM application instance name, either accept the default value of *Service Delivery* or enter a new value.
 - c. Enter the CA EEM administrator (EiamAdmin) password and click Next.

The installation program verifies the information that you entered and proceeds as follows:

- If the information is validated, the installation continues.
- If the information cannot be validated, the installation cannot continue. Before you resume the installation, verify whether CA EEM is installed. If necessary, install it. Also verify the server host name and password for accessing CA EEM.

7. Enter the [service provider business unit ID](#) (see page 37) and click Next.

This ID specifies the “root” business unit under which other business units or departments can be structured. As a best practice, specify your company domain name or a short version of your company name for the business unit ID.

8. Enter the Service View Web Server Startup and Shutdown port numbers or accept the defaults and click Next.

The installation begins installing components and configuring files.

9. Select Yes to restart your computer and click Finish, when prompted.

Restart your computer to help ensure that services start correctly and that all files are installed correctly.

You have installed the Service View server. You can optionally do the following:

- Install *additional* Service View servers
- Review the installation log files in %USM_HOME%\logs\install folder

If you have multiple installations of Service View, you can set up a [filestore](#) (see page 187) (a single location for shared files). Doing so helps improve overall system performance and helps reinforce best practices.

Install CA Service Catalog

Installing CA Service Catalog is a required task when you [install CA Service Catalog products and components](#) (see page 40).

Important! Install CA Service Catalog on the same computer as the *first* (formerly *primary*) Service View computer. The first Service View computer *must* be installed before you install CA Service Catalog.

Follow these steps:

1. Verify that the DBMS client (Oracle client or SQL Server client) is installed locally, unless the local computer is the DBMS server.

Note: For instructions to install the DBMS client, see your DBMS documentation.

2. Access the root folder on the CA Service Catalog installation media and run setup.exe.

The installation Product Explorer window appears.

3. Select CA Service Catalog, Product Install, Windows and click Install.
4. The installation wizard guides you through the installation process.
5. Click Finish when the setup wizard has completed.

You have installed CA Service Catalog. You can optionally review the installation log files in the %USM_HOME%\logs\install folder.

Installation of a Process Automation Tool

After you install CA Service Catalog, the installation program suggests that you install CA Process Automation as your process automation tool. You can optionally install CA Process Automation, [install CA Workflow](#) (see page 49), or install both. You can optionally use either or both of them to automate processes in CA Service Catalog. For best results, including more efficient process automation, install and use CA Process Automation rather than CA Workflow.

Note: For details about installing and using CA Process Automation, see the CA Process Automation documentation and installation media, which are included with the CA Service Catalog installation media. For details about using CA Process Automation with CA Service Catalog, see the *Integration Guide*.

Install CA Workflow

Installing CA Workflow as your process automation tool is an optional task when you [install CA Service Catalog products and components](#) (see page 40). You can optionally install CA Workflow on the *first* (formerly *primary*) Service View server or on other computers. In addition, you can optionally install CA Workflow on multiple computers. In such cases, consider using CA Workflow [clustering](#) (see page 21).

Note: For best results, including more efficient process automation, install and use CA Process Automation rather than CA Workflow. For details about installing and using CA Process Automation, see the CA Process Automation documentation and installation media, which are included with the CA Service Catalog installation media.

Follow these steps:

1. Verify that the DBMS client (Oracle client or SQL Server client) is installed locally, unless the local computer is the DBMS server.

Note: For instructions to install the DBMS client, see your DBMS documentation.

2. Access the root folder on the installation media and run setup.exe.

The installation Product Explorer window appears.

3. Select CA Workflow, Windows and click Install.
4. The installation wizard guides you through the installation process.

5. Enter the following database information:
 - If you are installing CA Workflow on the same computer as Service View, enter the password for the CA Service Catalog database user.
 - If you are installing CA Workflow on a different computer from Service View, select the database type, click Next, and then supply the following information:
 - For SQL Server, enter the SQL Server server name and other [parameters for the MDB on SQL Server](#) (see page 43).
 - For Oracle, enter the Oracle host name and other [parameters for the MDB on Oracle](#) (see page 44).

Answer the prompts and click Next.

6. Enter the CA EEM administrator (eIAM EiamAdmin) password and click Next.
7. Enter the startup and shutdown ports for CA Workflow or accept the defaults and click Next.
8. Click Finish after the setup wizard has completed.

You have installed CA Workflow. You can optionally review the installation log files in the %USM_HOME%\logs\install folder.

Note: The CA Workflow installation installs some workflow actors and process definitions. Some process definitions use “_EX_” in the name and are meant to serve as examples for your reference; their status is set to inactive. Configure CA Workflow for use with CA Service Catalog; for details, see the *Integration Guide*.

Install Catalog Content

Installing Catalog Content is a required task when you [install CA Service Catalog products and components](#) (see page 40). The Catalog Content supplies the default services, service options, and services option elements in the catalog. Install the Catalog Content on the *first* (formerly *primary*) Service View server *after* CA Service Catalog is installed.

Follow these steps:

1. Verify that the DBMS client (Oracle client or SQL Server client) is installed locally, unless this computer is the DBMS server.

Note: For instructions to install the DBMS client, see your DBMS documentation.

2. Delete old content from the catalog, if applicable. This step applies *only* if you performing a new installation as part of migration model upgrade or a traditional model upgrade.

The existing content is deleted so that you can install the updated content for existing services and folders.

Note: Attempting to install content that would replace an existing same-named folder or service in your catalog causes the installation of the entire folder to fail. For example, suppose the name of a subfolder or service in the IT Support Services folder duplicates a folder or service already in your catalog. In that case, *no* services or subfolders in the IT Support Services folder are installed. However, other folders and services whose names are *not* duplicated in your existing catalog are installed.

3. Access your CA Service Catalog installation media and run setup.exe.

The installation Product Explorer window appears.

4. Select CA Service Catalog, Best Practices Content: Foundation, Windows and click Install.
5. The installation wizard guides you through the installation process; you can select from a set of high-level folders of services.
6. Click Finish when the setup wizard has completed.

You have installed the Catalog Content. You can optionally review the installation log files in the %USM_HOME%\logs\install folder.

Install CA Service Accounting

Installing CA Service Accounting is an optional task when you [install CA Service Catalog products and components](#) (see page 40). You can optionally install CA Service Accounting multiple times on multiple computers, including the *first* (formerly *primary*) Service View server.

Follow these steps:

1. Verify that the DBMS client (Oracle client or SQL Server client) is installed locally, unless the local computer is the DBMS server.
Note: For instructions to install the DBMS client, see your DBMS documentation.
2. Access your CA Service Catalog installation media and run setup.exe.
The installation Product Explorer window appears.
3. Select CA Service Accounting, Windows and click Install.
Answer the prompts and follow the installation wizard.
4. Do *one* of the following, whichever is applicable:
 - If you *are* installing CA Service Accounting on a Service View computer, select the destination folder or accept the default and click Next.
 - If you are *not* installing CA Service Accounting on a Service View computer, do the following:
 - a. Select the database type, click Next, and do *one* of the following:
For SQL Server, enter the SQL Server host name, listen port, instance name, and database user ID and password.
For Oracle, enter the Oracle host name, service name, installation connection ID, listen port, and database user ID and password.
 - b. Enter the CA EEM administrator (EiamAdmin) password and click Next.
5. Click Finish when the setup wizard has completed.

You have installed CA Service Accounting. You can optionally review the installation log files in the %USM_HOME%\logs\install folder.

Installation and Configuration Procedures for Third-Party Unicode Fonts

Installing and configuring third-party Unicode fonts is a possible task when you [install CA Service Catalog products and components](#) (see page 40), as follows:

- If you do *not* need to enable Report Data Views to support double-byte characters in PDF export, skip this task.
- To enable Report Data Views to support double-byte characters in PDF export, do the following:
 - Install third-party Unicode fonts on all Service View computers, both the *first* (formerly *primary*) and any *additional* (formerly *secondary*) Service View computers
 - Configure CA Service Catalog to support these fonts

Note: For details about installing the third-party Unicode fonts and configuring CA Service Catalog to support them, see the `readme.txt` file in the `%USM_HOME%\view\conf\font-files` folder.

Chapter 4: Upgrading

This section contains the following topics:

[Traditional and Migration Model Upgrades](#) (see page 55)

[Scope and Limitations of an Upgrade](#) (see page 56)

[Prepare for the Upgrade](#) (see page 57)

[How to Upgrade Using a Migration Model](#) (see page 61)

[How to Upgrade Using a Traditional Model](#) (see page 63)

[Finalize the Upgrade](#) (see page 68)

Traditional and Migration Model Upgrades

You can upgrade CA Service Catalog to Release 12.7 using *either* a migration model or a traditional model.

- In a traditional model, you run the upgrade program on existing CA Service Catalog computers.
- In a migration model, you install CA Service Catalog 12.7 products and components on *new* computers. When you install CA Service Catalog on the new computers, you use the existing CA MDB and CA EEM computers.

The migration model provides greater flexibility than the traditional model. If a system failure or other unforeseen event occurs in the new environment, you can more efficiently restore the previous environment. In many cases, you can test the new environment more thoroughly when you use the migration model.

The [scope and limitations of an upgrade](#) (see page 56) include both general and release-specific requirements for traditional and migration model upgrades.

Similarly, the tasks to [prepare for the upgrade](#) (see page 57) apply to both traditional and migration model upgrades.

Scope and Limitations of an Upgrade

Important! Read and understand the scope and limitations of the upgrade *before* performing the upgrade!

The scope and limitations of the upgrade are as follows:

- If you are running CA Service Catalog r12.6, you can upgrade to CA Service Catalog 12.7 using *either* a traditional model or a migration model.
- If you are running CA Service Catalog r12 or r12.5, the same options apply. However, you *first* upgrade to CA Service Catalog r12.6 before upgrading to CA Service Catalog Release 12.7.

Important! If this option applies, [contact Technical Support](#) (see page 4) to obtain the CA Service Catalog r12.6 installation media, including its documentation. To perform this upgrade, follow the instructions from Technical Support, the *Implementation Guide*, and *Release Notes*.

- Upgrade *all or no* existing installations of the CA Service Catalog products and components. If you upgrade any CA Service Catalog component on any computer, upgrade *all other* existing CA Service Catalog components on that computer and on any other computers.
- Verify that CA Service Catalog [supports your database management system](#) (see page 32); if necessary, update your database management system to a supported version.

You *cannot* upgrade from one DBMS to another. For example, you cannot upgrade a CA Service Catalog r12.6 installation running SQL Server to a CA Service Catalog Release 12.7 installation running Oracle.

- This item applies to traditional model upgrades *only*. When you upgrade a computer that already has CA Service Catalog components from a previous release installed, you cannot install any *new* CA Service Catalog component on that computer. A *new* component is one that has not been installed previously. However, you can install the new component on a different computer.

For example, suppose Computer A has Service View, CA Service Catalog, and Catalog Content r12.6 installed. When you upgrade Computer A, you upgrade only those components to Release 12.7. You cannot install a new component, such as CA Service Accounting Release 12.7, on Computer A. Instead, install CA Service Accounting Release 12.7 on a computer that has no existing CA Service Catalog components installed.

- You *cannot* change locale operating systems when you upgrade. For example, you *cannot* upgrade a CA Service Catalog r12.6 installation on an English operating system to a CA Service Catalog Release 12.7 installation on a Japanese system.
- Service View upgrades can take a significant amount of time on Windows 2008 computers.

Prepare for the Upgrade

Preparing for the upgrade is a required task whether you upgrade using a [migration model](#) (see page 61) or a traditional model.

Follow these steps:

1. Review the [scope and limitations of an upgrade](#) (see page 56) for requirements regarding upgrades from specific earlier releases of CA Service Catalog.

Important! Read and understand the scope and limitations of the upgrade *before* performing the upgrade!

2. Find and list all computers in your implementation that have one or more CA Service Catalog components installed. Use this list to help verify that you upgrade all required computers efficiently and in the correct sequence. If necessary, work with other CA Service Catalog administrators and users to verify that your list is accurate and complete.
3. Do the following in your current implementation:
 - a. Log in to the root (highest level) business unit and click Service Builder, Configuration, Catalog Configuration.
 - b. Record whether the Use Service Provider Catalog Only option is set to Yes or No.
 - c. Decide whether to continue to use this value to use as a system setting to meet the requirements of your organization.

The Use Service Provider Catalog Only option is a [System Configuration option](#) (see page 185). Therefore, this option applies to the root business unit *only*, not any sub business units. You set this system value later at the end of the upgrade process.

4. Stop all CA Service Catalog Windows services. These services are named as follows:
 - Event Log Watch
 - CA Service View
 - CA Service Accounting
 - CA Service Fulfillment
 - CA Service Repository Agent
 - Message Queue 4.1 Broker
5. Review whether you have shared any of the folders under CA Service Catalog and Shared Components. If the folders are shared, unshare them before the upgrade and restore the share after the upgrade is finished.

Note: For details about sharing and unsharing, see your Windows documentation.

6. Verify that your *user ID* is defined as an administrator with *elevated privileges* on each *applicable Windows computer*.

user ID

Specifies your administrative user ID for the Windows computer (*not* your user ID for CA Service Catalog).

elevated privileges

Are additional rights in Windows that are available to administrative users only. To install or upgrade CA Service Catalog, administrators require the elevated privilege named Log on as Service.

applicable Windows computer

Specifies a Windows computer on which you plan to install or upgrade CA Service Catalog and which supports elevated privileges for administrators. An example is a Windows Server 2008 computer that has Service View, CA Service Catalog, and the Catalog content installed.

7. Verify that your administrative user ID has Log on as Service rights on each applicable Windows computer, as follows:
 - a. Click Start, All Programs, Administrative Tools, Local Security Policy, Security Settings, Local Policies, User Rights Assignment, Log on as Service.
 - b. Verify that your administrative user ID is listed. If it is not listed, complete the next step.
8. If necessary, assign Log on as Service rights to your administrative user ID on each applicable Windows computer, as follows:
 - a. Right-click the CA Service View Window Service (if installed). Select the Properties, Log on tab, and enter your administrator account credentials.
 - b. Perform the previous step for CA Service Accounting and CA Service Fulfillment, if applicable.

Note: These services can be installed on CA Service Catalog computers *without* Service View.
 - c. Restart the service.

A message appears stating that the administrator has been granted the Log on as a Service right.

9. If you have an existing filestore that you want to continue using after the upgrade, do the following. Otherwise, skip this step.
 - a. Back up the filestore.
 - b. Record the computer name and the complete pathname of the filestore. Save them for reference after the upgrade.
10. Do the following in your current implementation:
 - [Prepare the MDB and the DBMS](#) (see page 59).
 - [Back up CA EEM data](#) (see page 60).

You have prepared for the upgrade.

Prepare the MDB and the DBMS

Preparing the MDB and the DBMS is a required task whether you upgrade using a [migration model](#) (see page 61) or a traditional model.

Follow these steps:

1. Back up your existing CA MDB on the computer where it currently resides.
Note: For instructions to back up CA MDB, see your DBMS documentation.
2. (Recommended) Clean the `usm_system_change_detail` database table, as explained in this step and the next step.

These steps are optional and are recommended to help improve the performance of the product. These steps can require from several minutes to an hour, depending on the volume of the data in the table.

- a. Run the following command:

```
select * into usm_system_change_detail_temp from usm_system_change_detail where  
old_value!=new_value
```

This command copies the required data to a temporary table.

- b. Back up the script for all constraints for the following tables:
 - `usm_system_change_detail`
 - `usm_system_change_detail_ext`

3. Do the following, if you performed the previous step:
 - a. Drop the foreign key constraints for the `usm_system_change_detail_ext` table.
 - b. Drop the `usm_system_change_detail` table.
 - c. Rename the `usm_system_change_detail_temp` table to `usm_system_change_detail`.
 - d. Use the script that you backed up in the previous step to create indexes for the `usm_system_change_detail` and `usm_system_change_detail_ext` tables.
4. If applicable, on your DBMS server, upgrade your Oracle or SQL Server software to a supported version: Oracle 10g or 11g or SQL Server 2005 or 2008.
5. Verify that the Oracle or SQL Server client software is installed on each *required* computer. The version installed on the client must match the version installed on the DBMS server.

The *required* computers are the new CA Service Catalog computers, on which you plan to install or upgrade one or more CA Service Catalog products or components.

6. Remove replication in your DBMS.

Important! When replication has been added, the database tables are locked from any schema changes, even if replication is turned off. As a result, the upgrade cannot run successfully.

Note: For instructions to remove replication, see your DBMS documentation. Also see that documentation for instructions to add it again, after you have completed the upgrade.

You have prepared the MDB and the DBMS.

Back Up CA EEM Data

Backing up CA EEM data is a required task whether you upgrade using a [migration model](#) (see page 61) or a traditional model.

Follow these steps:

1. Back up your existing CA EEM on the computer where it currently resides, as follows:
 - a. If other CA Service Catalog components exist on the same computer, shut down their Windows services.
 - b. Log in to CA EEM; on the login page, select CA Service Catalog Release 12.7 as the application.
2. Click Configure, EEM Server.

The EEM Server options appear on the left side of the page.

3. Click Export Application.

The Export Application section appears on the right side of the page.

4. Do the following:

- a. Select all check boxes under Object List, and verify that Override the Max Search Size is *not* selected.

If CA EEM is configured with External Directory, clear these options: Global Users, Global User Groups, Global Folders, and Global Settings.

- b. Click Export.

- c. On the File Download prompt, select a location to save the ServiceCatalog.xml file. Record the location where you saved the file, for future reference.

5. Log out of CA EEM.

Note: For further details about backing up CA EEM, see your CA EEM documentation.

6. Back up the CA EEM data on the Service View computer in your test system, as follows.

Note: If you have multiple Service View computers, perform this step on the *first* (formerly *primary*) Service View computer *only*. You run this command once, regardless of how many Service View computers your system has.

- a. Open the CA Service Catalog command prompt by clicking Start, Programs, CA, Service Catalog, Service Catalog Command Prompt.
- b. Run the following command at the command prompt:

```
ant backup-eem-app
```

This action generates a file named eem-backup.xml in the %USM_HOME% directory.

You have backed up CA EEM data.

How to Upgrade Using a Migration Model

In a migration model upgrade, you install CA Service Catalog products and components on new computers. When you install CA Service Catalog on the new computers, use the existing CA MDB and CA EEM computers. To upgrade using a migration model, follow this process:

1. [Prepare for the upgrade](#) (see page 57).
2. Review the [guidelines for migration model upgrades](#) (see page 62). Follow them while installing the CA Service Catalog products and components.

3. [Install CA Service Catalog products and components](#) (see page 62).
4. [Finalize the upgrade](#) (see page 68).

You have upgraded using a migration model. You are now ready to [configure](#) (see page 97) CA Service Catalog before using it.

Also, optionally consider implementing [clustering](#) (see page 21) for Service View, CA Workflow, or both.

More information:

[New Installation, Upgrade, or Migration](#) (see page 27)

Guidelines for Migration Model Upgrades

Reviewing these guidelines is a required task when you [upgrade using a migration model](#) (see page 61). During a migration model upgrade, you [install CA Service Catalog products and components](#) (see page 62) on your new CA Service Catalog computers. During these installations, follow these guidelines:

- When you are prompted for information about CA MDB or CA EEM, use the *existing* CA MDB specifications. These specifications include the usmuser and CA EEM values (such as the computer and application names).
- Consider this sample scenario: Your setup has Service View and CA MDB on existing Computer 1, CA Service Catalog and CA Service Accounting on existing Computer 2, and CA Workflow on existing Computer 3. Do the following:
 - Verify that CA Service Catalog supports the DBMS version on existing Computer 1.
 - Verify that the DBMS client software is installed on all required computers.
 - Do *not* upgrade or delete the Service View on existing Computer 1. Instead, install Service View on new Computer 4, pointing to the existing CA MDB on existing Computer 1. Similarly, install CA Service Catalog and CA Service Accounting on new Computer 5, and install CA Workflow on new Computer 6.

How to Install CA Service Catalog Products and Components

Installing CA Service Catalog products and components is a required task when you [upgrade using a migration model](#) (see page 61).

1. Review the [guidelines for migration model upgrades](#) (see page 62). Follow them while installing the CA Service Catalog products and components.
2. [Install CA EEM](#) (see page 41).

3. Install the *first* (formerly *primary*) Service View computer. The installation program installs Service View and upgrades the MDB as part of this procedure.
4. (Optional) Install *additional* (formerly *secondary*) Service View computers.
5. [Install CA Service Catalog](#) (see page 48).
6. (Optional) Install CA Process Automation (the recommended process automation tool), [install CA Workflow](#) (see page 49), or install both.

Note: For details about installing and using CA Process Automation, see the CA Process Automation documentation and installation media, which are included with the CA Service Catalog installation media.

7. [Install Catalog Content](#) (see page 51).
8. [If applicable, install CA Service Accounting](#) (see page 52).

Note: If you plan to integrate CA Service Catalog with any other CA product, see the *Integration Guide*.

You have installed CA Service Catalog products and components.

How to Upgrade Using a Traditional Model

In a traditional model, you run the upgrade program *only* on existing CA Service Catalog computers. To upgrade CA Service Catalog using a traditional model, do the following:

1. [Prepare for the upgrade](#) (see page 57).
2. [Upgrade CA EEM](#) (see page 64).
3. Find and record the values of the following MDB parameters for your DBMS and have them ready when you upgrade the first Service View server:
 - [Parameters for the MDB on SQL Server](#) (see page 43)
 - [Parameters for the MDB on Oracle](#) (see page 44)

This data is the same data required for a new installation of the MDB. Even if you do not need to upgrade the MDB, verify the MDB version and the related parameter values to help verify the database configuration.

When you start upgrading the *first* (formerly *primary*) Service View computer, the installation checks whether to update the MDB, and proceeds as follows:

- If the MDB installation or upgrade starts, you are prompted to supply the required parameter values. Examples include the server name and the logon credentials for your DBMS:
- If the MDB upgrade is not necessary, it is not started. You proceed directly to upgrade the CA Service Catalog products and components.

4. [Upgrade Service View and other products and components](#) (see page 65), as directed by the installation program.

The installation program guides you through this entire process on all computers.

5. [Finalize the upgrade](#) (see page 68).

You are now ready to [configure](#) (see page 97) CA Service Catalog before using it. Also, optionally consider implementing [clustering](#) (see page 21) for Service View, CA Workflow, or both. Also, if you have multiple installations of Service View, you can [set up a single location for shared files](#) (see page 187). Doing so helps improve overall system performance and helps reinforce best practices.

Note: If you are using CA Workflow, we recommend the following for more efficient process automation: After you upgrade your existing CA Workflow implementation, install and use CA Process Automation rather than CA Workflow. For details about installing and using CA Process Automation, see the CA Process Automation documentation and installation media, which are included with the CA Service Catalog installation media.

More information:

[Choose New Installation, Upgrade, or Migration](#) (see page 27)

Upgrade CA EEM

CA EEM authenticates users during login and authorizes users to access CA Service Catalog.

Follow these steps:

1. Review the [installation considerations](#) (see page 41).
2. Shut down the Windows service for CA EEM.
The service name can be iTechnology Gateway or CA iTechnology Gateway.
3. Start the setup.exe file on the CA Service Catalog installation media.
The Product Explorer window of the installation program appears.
4. Select Utilities, CA EEM, Windows, and click Install.
The installation wizard guides you through the installation process.
5. Enter the value of the EiamAdmin password that you want to use, when prompted.
Record this password for future reference.

6. When you are prompted for the Java Home directory, leave the value empty and click Skip, unless you plan to do one or both of the following:

- Integrate CA EEM with CA SiteMinder
- Use Security Assertions Markup Language (SAML) with CA EEM

If you plan to perform either of these tasks, enter the complete path name of your Java Runtime Environment (JRE) installation.

7. Continue following the wizard instructions and complete the CA EEM installation.
8. Reinstall CA Anti-Virus or CA Threat Manager, if you uninstalled it earlier.

You have installed CA EEM.

Note: For instructions to configure and use CA EEM, see the *Integration Guide*.

Upgrade Service View and Other Products and Components

When you [upgrade using a traditional model](#) (see page 63), upgrading Service View and related products and components is a required task. The upgrade program guides you through the upgrade of the MDB (if applicable), the first Service View computer, and other products and components.

Important! If Service View is installed on multiple computers, upgrade the *first* (formerly *primary*) Service View computer first, and then upgrade all *additional* (formerly *secondary*) Service View computers. Upgrading the first Service View computer *before* upgrading any additional Service View computers is critical! If you do not do so, the upgrade aborts!

Follow these steps:

1. On the first Service View computer (if applicable), open the CA Service Catalog Product Explorer, select Service View, Windows.

The Component Information field in the Product Explorer displays text informing you that this component (Service View) is already installed.

2. Click the Install button.

The installation program verifies that this computer is the first Service View server.

3. When you are prompted to confirm that you want to upgrade the existing version of Service View, click Yes.

The installation program uninstalls the existing versions of Service View and any other local CA Service Catalog products or components (CA Service Catalog, Catalog Content, CA Service Accounting, and CA Workflow). The installation program then starts installing the new version of Service View.

4. Follow the prompts to complete the new installation of Service View.

When you start upgrading the *first* (formerly *primary*) Service View computer, the upgrade program starts the MDB upgrade automatically, if applicable.

- a. Supply the required parameter values for your DBMS, if the MDB upgrade is started, as follows:

- [Parameters for the MDB on SQL Server](#) (see page 43)
- [Parameters for the MDB on Oracle](#) (see page 44)

You recorded these values earlier while reviewing how to upgrade using a traditional model.

If the MDB upgrade is not needed, it is not started, and the Service View upgrade continues.

- b. If Service View is installed on multiple computers, upgrade the first Service View server, as directed by the installation program.

During the upgrade of the first Service View computer, the installation program uninstalls all additional existing CA Service Catalog components on the first Service View computer. These components include CA Service Catalog and Catalog Content (Best Practices Foundation), and can include CA Service Accounting and CA Workflow.

After the upgrade of the first Service View computer finishes, the Product Explorer does the following:

- Displays the names of the CA Service Catalog components that were uninstalled from the first Service View computer and prompts you to install new versions of these components.

For example, suppose the computer with the first Service View also has CA Service Catalog, Catalog Content, CA Service Accounting, and CA Workflow installed. In that case, the installation program uninstalls them when you upgrade to the new version of Service View. After that Service View upgrade is finished, the installation program prompts you to install the new versions of CA Service Catalog, Catalog Content, CA Service Accounting, and CA Workflow.

- Detects and displays but does *not* uninstall all existing CA Service Catalog components that are installed on the computers other than the first Service View computer. These components can include one or more installations of CA Service Accounting and CA Workflow, and can include one or more additional Service View installations.

5. Note these installations of CA Service Catalog components on this computer and other computers on your network and save them for reference throughout this upgrade process.

6. Install CA Service Catalog locally on the first Service View computer, as follows:
 - a. Select CA Service Catalog on the Product Explorer and click Install.
 - b. Follow the prompts to complete the new installation.
 - c. Select Catalog Content (Best Practices Foundation) on the Product Explorer and click Install.
 - d. Follow the prompts to complete the new installation.

Note: CA Service Catalog is required on the first Service View computer. CA Service Catalog cannot be installed on any computer except the first Service View computer.

After this installation finishes, a confirmation message appears.

7. (Optional) Install CA Workflow locally on the first Service View computer, if applicable. Otherwise, skip this step.
 - a. Select CA Workflow on the Product Explorer and click Install, if applicable. Otherwise, skip this step.
 - b. Follow the prompts to complete the new installation of CA Workflow.

After this installation finishes, a confirmation message appears.

8. (Optional) Install CA Service Accounting locally on the first Service View computer, if applicable. Otherwise, skip this step.
 - a. Select CA Service Accounting on the Product Explorer and click Install.
 - b. Follow the prompts to complete the new installation of CA Service Accounting.

After this installation finishes, a confirmation message appears.

You are finished upgrading CA Service Catalog products and components on the first Service View computer.

9. Upgrade the remaining CA Service Catalog components in your network, one computer at a time, as follows:
 - Reference the information displayed earlier about the installations of Service View, CA Workflow, and CA Service Accounting on computers in your network *other than* the first Service View computer. The Product Explorer displays this information after the installation of the first Service View computer.
 - Upgrade all existing components on all these remaining CA Service Catalog computers.

You have upgraded Service View and other CA Service Catalog products and components.

Finalize the Upgrade

Finalizing the upgrade is the last required task when you [upgrade using a migration model](#) (see page 61) or [upgrade using a traditional model](#) (see page 63).

Follow these steps:

1. Log in to the root business unit of CA Service Catalog as a Service Delivery administrator.
2. Do the following:
 - a. Click Service Builder, Configuration, System Configuration.
The [System Configuration options](#) (see page 185) appear.
 - b. Set the value of the Use Service Provider Catalog Only option to Yes or No. You decided the value at the beginning of this upgrade process.
Note: The value you set applies to the entire Catalog system, in other words, to all business units.
3. Verify that you and other users can log in to CA Service Catalog on the new computers. Verify that the CA Service Catalog components are working properly.
4. If you have installed or upgraded CA Workflow as part of the upgrade process, [configure CA Workflow](#) (see page 71).
5. If you integrated CA Service Catalog with CA Service Desk Manager in the previous release, update the host computer names. Also reconfigure the other connection details between the two products.
Note: For instructions, see the *Integration Guide*.
6. [Enable Windows NTLM authentication](#) (see page 105), if you enabled in the previous release.
Important! This option is disabled by default, for both new installations and upgrades. If applicable, enable it again.
Windows NTLM authentication is enabled.
7. [Set up shared and customized files](#) (see page 69).
8. (Multiple Service View computers) Do the following:
 - a. If you have not already done so, set up the [filestore](#) (see page 186) (the single location for shared files).
 - b. Click Administration, Configuration, Filestore on any Service View computer. Verify that the filestore location is correct. If necessary, correct the location.
 - c. Access the filestore computer and verify that the filestore folder includes the themes folder. If necessary, copy the themes folder to the filestore folder, as explained in the next step.

9. To use the old filestore location, do the following. Otherwise, skip this step.
 - a. Copy the themes folder from the local filestore to the old filestore. This folder is part of the new feature named [custom branding](#) (see page 309).
Note: The themes folder is new with this release.
 - b. Click Administration, Configuration, Filestore.
 - c. Specify the original filestore location. You recorded this location before the upgrade.
10. (Migration model upgrades only) [Uninstall](#) (see page 331) the previous versions of CA Service Catalog products and components from the "old" CA Service Catalog computers. If you installed a new version of CA EEM, uninstall the old version of CA EEM from the old CA Service Catalog computers.

You have finalized the upgrade.

How to Set Up Shared and Customized Files

Setting up shared and customized files is a required task when you [finalize the upgrade](#) (see page 68).

To set up shared and customized files

1. Copy all filestore contents (files shared by all users in the environment) from the previous filestore location to the new location, as follows:
 - Documents: Copy from %USM_HOME%\view\documents to %USM_HOME%\filestore\documents
 - Images: Copy from %USM_HOME%\view\webapps\usm\images\offerings to %USM_HOME%\filestore\images\offerings
 - Images: Copy from %USM_HOME%\view\webapps\usm\images\rateplans to %USM_HOME%\filestore\images\rateplans
 - Forms: Copy from %USM_HOME%\view\forms to %USM_HOME%\filestore\forms
 - Custom directory: Copy any files that you want to update or replace from %USM_HOME%\view\webapps\usm\custom to %USM_HOME%\filestore\custom

Note: Your installation can have some or all of these folders, depending on the previous version of CA Service Catalog that was installed.

2. If you customized files, such as category.xml or requestshared.xml, restore or verify your customizations, as follows:

- (Migration model upgrade only) Compare each customized file that you backed up earlier with the new version supplied by the upgrade. Update the new file with your customizations from the backup file.

Important! You can replace certain new files with your backup files, in certain cases. However, *before* doing so, contact Technical Support and verify each file that you want to replace. For details, [contact Technical Support](#) (see page 4).

- (Traditional upgrade only) Review any CA Service Catalog files that you customized, such as custom.xml or requestshared.xml. Verify that your customizations are intact and are applicable for this release.

The traditional upgrade program automatically backs up customized files before the upgrade and restores them after the upgrade.

3. Do the following if you customized the CA Service Repository Agent in the previous release and you want to use the same customizations for the new release.

Note: The CA Service Repository Agent is also named the Data Mediation Data Repository Agent. This repository agent automates the process of importing usage data stored in Delimiter Separated File or Fixed Length File format.

- a. Find the files from the previous release. These files are located in the following folders:

- %USM_HOME%\Repagent\data
- %USM_HOME%\Repagent\config

- b. Open each file and find the customizations that you want to continue using. Make the same or equivalent customizations to the files with the same names in the new folders. The new folders are as follows:

- %USM_HOME%\Repagent\data
- %USM_HOME%\Repagent\config

Important! Do *not* simply overwrite the new files with the old files. Doing so does *not* work.

- c. Complete these updates for the *first* (formerly *primary*) Service View computer.
- d. Complete these updates for any *additional* (formerly *secondary*) Service View computers.

You have set up shared and customized files.

Configure CA Workflow

If you are using CA Workflow, configure its parameters, actors, and process definitions when you [finalize the upgrade](#) (see page 68).

Follow these steps:

1. Do the following on each newly upgraded Service View server:
 - a. Log in to CA Service Catalog.
 - b. Click Administration, Configuration, CA Workflow.
The [CA Workflow configuration parameters](#) (see page 121) appear.
 - c. Verify that these parameters reference the newly upgraded CA Workflow computer. If necessary, update these parameters to match the newly upgraded CA Workflow computer.
2. Configure the CA Workflow actors, as follows:
 - a. On the CA Service Catalog GUI, select Administration, Configuration, CA Workflow.
 - b. Click Configure.
The Workflow actors are configured.
3. (Only for upgrades from CA Service Catalog r12 or earlier) Update the URL in every process definition that you plan to use with CA Service Catalog to point to the newly upgraded first Service View server: In each of these process definitions, select the Initialize Values function and set the USM_URL to reference the newly upgraded first Service View server.
Note: The first step of this procedure changes the URL of the actors only, *not* the process definitions.
4. Review the process definitions that you activated in the previous release. If you want to use the new process definitions from the new release, do the following:
 - a. Make the process definitions from the previous release inactive and activate the equivalent process definitions supplied with the new version of CA Service Catalog.
 - b. If you customized the previous process definitions, make the same customizations to the new process definitions.

Note: For assistance, see the CA Workflow IDE online help.

5. (Only for integrations of CA Service Catalog with CA Service Desk Manager) Do the following on the CA Workflow IDE for CA Service Desk Manager:
 - a. Import the USM_RequestService web service actor from %USM_HOME%\fulfillment\scripts\actors.
Note: This action is required because the former %USM_HOME%\fulfillment\scripts\service_desk\actors folder has been removed from the installation program.
 - b. Verify that the USM_URLs in the process definitions imported from CA Service Catalog point to the first CA Service Catalog computer.

You have upgraded the CA Workflow actors and process definitions.

Chapter 5: Migrating

This section contains the following topics:

[Migration](#) (see page 73)

[Disaster Recovery](#) (see page 74)

[How to Perform Prerequisite Tasks](#) (see page 74)

[How to Migrate](#) (see page 75)

Migration

You can migrate CA Service Catalog from one system to another system, to replicate your environment. Typically, you perform such a migration to move from a test system to a production system or as part of disaster recovery procedures. You can also perform such a migration as part of upgrading using a migration model.

For clarity, this documentation uses these terms:

- *test system* refers to all computers *from* which you are migrating
- *production system* refers to all computers *to* which you migrating

Thus, this documentation uses these terms to describe a typical scenario, migrating from a test system to a production system. If you are migrating for other reasons, the test system is the *source* system and the production system is the *target* or *destination* system.

This documentation assumes a multicomputer setup. For example, the "medium architecture" system referenced in [System Architecture](#) (see page 14) consists of three computers: one computer for the DBMS (including the MDB), one computer for CA Service Catalog and CA Service Accounting and one computer for CA Workflow. Unless indicated otherwise, *system* refers to *all* CA Service Catalog computers in your test or production system, including the DBMS computer. If you are migrating one stand-alone CA Service Catalog system to another stand-alone system, ignore references to multiple computers.

Note: For information about migrating a product that integrates with CA Service Catalog, see its documentation. For example, for information about migrating CA Process Automation, see the CA Process Automation documentation. Similarly, for information about migrating CA Service Desk Manager, see the CA Service Desk Manager documentation.

Disaster Recovery

The main goal of [migrating](#) (see page 75) a CA Service Catalog installation from one system to another system is to replicate your environment in a new setting. The goals and instructions for migrating also apply to both standard test-to-production updates and disaster recovery.

How to Perform Prerequisite Tasks

Perform the following prerequisite tasks before you [migrate](#) (see page 75) CA Service Catalog. These tasks are required to help ensure that you can complete the migration process successfully.

1. Verify that the setup on the production system matches the setup on the test system. In other words, verify that the production system has CA Service Catalog installed on the same number of computers as the test system. Verify that the same products and components are installed on each computer in the production system as its "matching" computer in the test system.

Thus, each test computer must have a matching production computer, and both of these computers must have the same CA Service Catalog components installed.

For example, suppose the first test computer has installed Service View, CA Service Catalog, the Catalog Content (Best Practices Foundation), and CA Service Accounting. In that case, the first production computer must also have each of these components installed. Moreover, the production computer must not have any *additional* CA Service Catalog products and components installed.

2. Plan your migration. You migrate from the old system to the new system incrementally in pairs. Each increment consists of a migration process from one test computer to the "matching" production computer.
3. Verify that the business unit ID of the service provider is *the same* in both systems.

Important! The service provider business unit ID for the new installation *must match* the previous installation.

4. Verify that all computers in both systems are at the same patch level for all important software. Examples include the DBMS, the MDB, any patches for CA Service Catalog products and components, including CA EEM, and so forth.
5. Verify that the CA EEM Application Name for CA Service Catalog is the same on both the test and production systems. By default, this name is *Service Catalog*.

If necessary, update the Application Name, on either or both systems. For instructions, see your CA EEM documentation.

6. Back up an existing data that you want to keep for use after the migration, and copy the backed up data to a different computer. Any existing data is overwritten during the migration process.

7. Using the Windows Control Panel, stop the CA Service Catalog services on all CA Service Catalog computers: CA Service View, CA Service Accounting, CA Service Fulfillment, and Message Queue 4.1 Broker.
8. Back up the MDB of your *production* system, on the computer where the MDB is installed. This requirement applies, regardless of whether the system is installed on one computer or multiple computers.

For instructions to back up the database, see your DBMS documentation.
9. Back up the MDB database of your *test* system, on the computer where the MDB is installed. This requirement applies, regardless of whether the system is installed on one computer or multiple computers.

You have performed the prerequisite tasks for migrating CA Service Catalog.

How to Migrate

You migrate CA Service Catalog products and components from one system to another for several reasons. Examples include upgrades, test-to-production moves, best practices, governance, security, or resource-related reasons. To migrate from one system to another, for example, from test to production, perform these tasks:

1. Restore the MDB database backup of the test system into your production system. You backed up this system while [performing the prerequisite tasks](#) (see page 74).

During this process, select the option for overwriting the existing MDB database.

For instructions to restore the database, see your DBMS documentation.
2. Unregister the CA EEM application used by the production system, as follows:
 - a. Log in to the Global Application of CA EEM as the EiamAdmin user
 - b. Select Configure, Applications, Service Catalog application.

If your systems use a different name than *Service Catalog* for the CA Service Catalog application name, use that name instead.
 - c. Click the UnRegister button.

3. Back up the CA EEM data on the Service View computer in your test system, as follows.

If you have multiple Service View computers, perform this step on the *first* (formerly *primary*) Service View computer. You run this command once, regardless of how many Service View computers your system has.

- a. Open the CA Service Catalog command prompt by clicking Start, Programs, CA, Service Catalog, Service Catalog Command Prompt.
- b. Run the following command at the command prompt:

```
ant backup-eem-app
```

This action generates a file named eem-backup.xml in the %USM_HOME% directory.

4. Copy the following files from the Service View computer in the test system to the Service View computer in the production system.

If you have multiple Service View computers, perform this step on the *first* (formerly *primary*) Service View computer in each system. You copy these files once, regardless of how many Service View computers your system has.

- %USM_HOME%\seeddata.properties
- %USM_HOME%\filestore folder

This folder may exist on a different computer than the current computer. To verify its location, select Administration, Configuration, Filestore Information. If no filestore location is specified, you do not need to copy this folder now. However, as a best practice, soon after the migration, [set up a single location for shared files](#) (see page 187).

- %USM_HOME%\eem-backup.xml

5. Open the %USM_HOME%\seeddata.properties file for editing and do the following:

- a. Update the value of the _USMHOME_ parameter with the complete folder name on the production computer of CA Service Catalog. For example:

```
_USMHOME_=C:/Program Files/CA/Service Catalog
```

- b. Update the value of the _IMQVARHOME_ parameter with the complete folder name on the production computer of the Message Queue 4.1 Broker. For example:

```
_IMQVARHOME_=C:/Program Files/CA/Service Catalog/view/conf/var
```

- c. Save your changes to the seeddata.properties file.

Note: When entering the folder names for these parameters, use the forward slash (/) not the backslash (\) as the separator character.

6. Run the following commands—in the order shown—on all CA Service Catalog computers in the production system.

Important! Run all the following commands on each computer, one computer at a time, until you have run them on all CA Service Catalog computers. For example: first, run all commands on computer1; next, run all commands on computer2; third, run all commands on computer3; and so on.

- a. `ant update-db-user`

This command enables you to [update the password of the database user](#) (see page 194). The command updates these password references globally to help ensure that CA Service Catalog continues to run efficiently throughout your environment.

Verify that the password you specify adheres to your organizational standards.

- b. `ant update-db-host`

This command enables you to update any or all of the following database settings: host name, port number, instance name, or service name. CA Service Catalog components use these settings to communicate with each other and the database.

Important! The database host name that you specify must be different than the one used in the test system. Updating the other settings is optional.

For details about this command, see [How to Update the Database Host, Port, Instance, or Service Names](#) (see page 196).

- c. `ant restore-eem-app`

This command restores the CA EEM database from the test system to the production system, using the `eem-backup.xml` that you copied earlier.

- d. `ant update-usm-host`

This command enables you to change the host name and port number for a computer running Service View, CA Workflow, or both.

Important! All host names for Service View and CA Workflow on the production system must be different from the ones in the test system. Updating the other settings is optional.

For details about this command, see [How to Update the Host Name and Port Number for Service View and CA Workflow](#) (see page 202).

7. Start all CA Service Catalog services on all computers in the production system. Using the Windows Control Panel, start these services: CA Service View, CA Service Accounting, CA Service Fulfillment, and Message Queue 4.1 Broker.
8. Log in to CA Service Catalog in the production system and do the following:

- a. Select Administration, Configuration, and update the configuration sections for the following:

Important! If your post-migration environment does *not* include any option in the list, update the configuration settings accordingly to *remove* the integration! Similarly, if your post-migration environment *does* include any of these options, do the following: Verify that the host names, port numbers, and other configuration data are correct for your post-migration environment. Remember that setting up a filestore location is a best practice, as mentioned earlier.

- Filestore
- CA Service Desk Manager integration
- CA CMDB integration
- CA Workflow

- b. Select Administration, Configuration, Workflow, and click Configure.

The actors are reconfigured to use the new environment.

9. Test by verifying that the same users, services, requests, and so forth that existed in the test system also exist in the production system.

You have migrated CA Service Catalog.

Chapter 6: Content Packs

This section contains the following topics:

[Overview of Content Packs](#) (see page 79)

[How to Manage Content Packs](#) (see page 80)

[Export Content Packs](#) (see page 81)

[Import Content Packs](#) (see page 84)

[Actions that You Can Perform on Imported Objects](#) (see page 85)

[Enable and Disable Content Packs](#) (see page 87)

Overview of Content Packs

A content pack is a collection of CA Service Catalog objects, such as services, Form Designer forms, policies, events, report data objects, CA Process Automation processes, and so forth. As a producer or designer, you create and export content packs to package customized versions of these objects efficiently and accurately. As a consumer or adopter, you import content packs so that you can use these customized objects without having to perform the same customization processes. Typically, the customizations in a content pack are focused on configuring your Catalog system for the optimal use of a specific feature, service, or environment. Content packs enable you to repeat these customizations efficiently and accurately from one system to another, multiple times.

Using content packs enables you to do *both* of the following:

- As a producer or designer of content packs, you package a library of objects, including your updates and customizations, in a single location.
- As a consumer or adopter of content packs, you import the customized objects programmatically in a single operation, as many times as necessary.

Consequently, you do not have to repeat individual operations for each object type. Content packs thus provide an efficient method of packaging and applying such updates and customizations, especially when you move from one implementation to another. Examples include the following:

- Test-to-production migrations and other same-release migrations
- Replacement of a decommissioned computer
- Restoring customizations after upgrading CA Service Catalog

Both customers and CA Technologies can create content packs, as follows:

- CA Technologies typically creates content packs that include new objects or updated versions of existing objects, including sample objects and fixes.
- Customers typically create content packs that include objects that they have customized to meet specific organizational requirements.
- Customers can optionally copy content packs from CA Technologies and customize them before applying them across their implementations.
- You can export and import multiple content packs for a single business unit. Similarly, you can export and import multiple content packs for all business units. If a conflict occurs between the existing content pack and the one you are activating, the new content pack auto overrides the old one.

The following roles are most likely to create and export content packs:

- Members of a CA Technologies content team
- A service delivery manager or other administrator in your organization

The most likely role to import a content pack is a service delivery manager or other administrator.

How to Manage Content Packs

To manage content packs, follow this process:

1. Test all content that you want to export, to verify that it works correctly (without errors). Also verify that it meets your requirements.
2. Create and [export the content pack](#) (see page 81) from an existing computer.
3. [Import the content pack](#) (see page 84) on a new computer.

Note: Content packs are always imported in an inactive state.

4. Review the [actions that you can perform on imported objects](#) (see page 85). If applicable, set the permissions or perform limited editing on the objects.
5. [Enable the content pack](#) (see page 87) in a business unit. If necessary, you can disable the content pack.

Note: If you copy and customize an object from a content pack, the customized object is *not* affected when you disable or reenables the content pack.

Export Content Packs

You create content packs to record (export) customizations so that you can reuse them in another implementation. For example, consider a test-to-production migration: You can reuse customizations by exporting a content pack on the test system and importing it on the production system. Using content packs provides greater efficiency and accuracy than repeating multiple customization processes manually.

Follow these steps:

1. Decide and record the objects that you want to include in the content pack.
You can include any or all of the following categories:
 - API plug-ins
 - CA Process Automation processes
 - Events, including rules, and actions
 - Form Designer forms
 - Policies
 - Report data objects
 - Services, including service hours and request SLAs
2. For each category that you select, decide and record which objects to include. You can do the following for each category. The ant command guides you through the selection process.
 - Include all objects in your implementation; that is, all objects in all business units (domains)
 - Include all objects from one or more specific business units only
 - Include only the objects that you specify by object names, for example, in a comma-separated list
 - Include only the objects that you specify by object-specific criteria
For example, for services, you can specify date last modified.

Note: Events, rules, actions, and report data objects (including API plug-ins) are *not* specific to any business units. That is, they always apply to *all* business units.

3. On the source computer, select Start, Programs, CA, CA Service Catalog, Service Catalog Command Prompt.

The CA Service Catalog command prompt opens.

4. Run the following command at this command prompt:

```
ant create-contentpack
```

The Catalog system creates the folder structure for the content pack.

The Catalog system also prompts you to specify the following:

- Basic identification data for the content pack, such as name, author, description, and so forth.
- The message with which to prompt the user during import.

5. Answer the prompts.

Note: We recommend that you name the *folder* to include the name, version, and locale (language) of the content pack.

The ant command creates the content pack folder named %USM_HOME%\FileStore\contentpacks*folder-name*.

This folder includes the contentpack.properties file. This file stores the identification data for the content pack.

This folder also contains several subfolders, including the following and others:

- Events
- Forms
- Policies
- Reports
- Services

If applicable, you populate these subfolders later in this procedure.

6. Answer the prompt about whether to export the objects into this content pack now or later, as follows:

- If you specify Yes, skip to the next step.
- If you specify No, run the following command on the source computer when you are ready:

```
ant export-to-contentpack
```

7. Answer the prompts about which objects to export, and their attributes. Use your answers to Steps 1 and 2 for reference.

The ant command does the following:

- Creates an XML file for each object that you specified, using the attributes that you specified
- In most cases, copies the XML file to the appropriate subfolder

For example, if you exported services, the ant command does the following:

- Creates a services.xml file using the attributes that you specified
- Copies the services.xml file to the Services subfolder of the content pack folder

The ant command copies some (but not all) categories of objects to their subfolders. Therefore, you copy the remaining categories of objects to their folders manually, as explained in the next step.

8. When prompted, copy the objects that you want to include (if any) to the following subfolders of the content pack folder depicted in Step 4:

Processes

Stores CA Process Automation processes.

Images\Offerings

Stores images for the services that you have included the Services subfolder.

Images\RatePlans

Stores images for the service option groups that you have included in the Services subfolder.

Prescripts

Stores custom scripts to run *before* you import the content pack. Examples include scripts that unzip files required for the import or scripts that display critical information.

Postscripts

Stores custom scripts to run *after* you import the content pack. Examples include scripts that load data into the Catalog system or that prompt the user for configuration specifications.

Plugins

Stores custom API plug-ins.

You have created the content pack on the source computer. You are now ready to import it on the target computer.

Import Content Packs

You import content packs so that you can reuse customizations that you (or another administrator) previously exported from another implementation. Using content packs provides greater efficiency and accuracy than repeating multiple customization processes manually.

Note: As a best practice, use scheduled down time, when no users are active on CA Service Catalog, to import, enable, or disable content packs.

Follow these steps:

1. Copy the content pack folder (%USM_HOME%\FileStore\contentpacks\folder-name folder) from the source computer to a location on the target computer. Record the location for reference.

2. On the target computer, select Start, Programs, CA, CA Service Catalog, Service Catalog Command Prompt.

The CA Service Catalog command prompt opens.

3. Run the following command at this command prompt:

```
ant import-contentpack
```

4. When prompted, enter the complete path name of the folder that stores the content pack to import.

The ant command displays the prompt message that you (or another administrator) specified when you created the content pack.

5. When prompted, do the following:

- a. Confirm that you want to continue the import.
- b. Enter the business unit ID for the content pack. You can specify any business unit, including the root business unit.
- c. Answer the object-specific prompts. When applicable, consider carefully whether to import objects as disabled.

For example, you import a new rule action that affects the emails that the Catalogs system sends. Before you enable the new rule action, you likely want to update the configuration of your mail server.

Note: If you import objects as disabled, you cannot use the objects until you enable them manually.

6. The ant command guides you through the remaining steps of the import.

7. If the content pack includes events, rules, or actions, restart the Windows service named CA Service View. Restart this service on *all* Service View computers in your environment.

Important! If you do not restart the CA Service View service on *all* Service View computers, unpredictable results can occur.

8. Test the import, as follows:
 - a. Log in to CA Service Catalog and select Service Builder, Configuration.
 - b. Click Content Packs in the left menu and select the content pack that you imported.
 - c. Verify the following:
 - The Content Pack Details section lists the details that you specified when you created the content pack, for example, the name, version, and status.
 - The Content section lists the object that you specified, according to the criteria that you specified.
 - d. Verify that the UI menus include the imported objects. For example, select Service Builder, Services and verify that the list of services includes any services that you imported. Similarly, select Administration, Tools, Events and verify that the list of events includes any services that you imported.

You have imported the content pack. All imported objects are either read-only or permit only limited editing.

Actions that You Can Perform on Imported Objects

The actions that you can perform on the objects imported from a content pack vary by object. When applicable, you perform certain actions on certain imported objects so that users can view and use the objects. The following table shows which actions apply to which objects.

Object	Enable or Disable	Set Permissions	Limited Editing
Services	Y	Y	Y
Service option groups	Y	Y	Y
Policies	Y	Y	Y
Events	N	Y	N
Rules	Y	Y	N
Actions	Y	Y	N
Forms	N	Y	N

Report data objects	N	Y	N
Images	N	N	N

The actions are as follows:

- [Enable or disable](#) (see page 87)

You enable objects so that users and the Catalog system can use them. For example, if your content pack includes policies, you enable these policies so that the Catalog system can use them as it manages requests. Similarly, if your content pack includes services, you enable these services so that users can view and request the services. For any reason, such as a problem occurring, you can disable any objects that you have enabled.

- Set permissions

To set permissions for each Catalog role on an imported object, use the portion of the UI that stores and maintains the object. For example, to set permissions for services, select Service Builder, Services, and edit the service details.

- Edit limited attributes

Typically, imported objects are read-only. You can perform only limited editing on certain imported objects, as follows:

- For services and service options, you can change the date available and date unavailable.
- For policies, you can add or subtract approvers, change the priority, and set the status as active or inactive.

Otherwise, to customize an imported object, copy and modify it. For example, to customize an imported report data object, copy and modify it. Similarly, to customize an imported rule or action, copy and modify it, as you would typically do to customize a predefined rule or action.

Note: For information about copying and modifying specific objects, see the *Administration Guide*.

Enable and Disable Content Packs

You can enable and disable either an entire content pack or individual objects (if applicable) in the content pack. You enable a content pack so that the Catalog system can use its objects. For example, if your content pack includes policies, you activate these policies so that the Catalog system can use them as it manages requests. Similarly, when applicable, users can view and use the objects that you enabled. For example, if your content pack includes services, you enable these services so that users can view and request the services. Enabling the imported objects and [setting permissions](#) (see page 85) on them work together to let users view and use the imported objects. After you enable objects in a content pack, you can disable them, for example, if a problem occurs.

Note: As a best practice, use scheduled down time, when no users are active on CA Service Catalog, to import, enable, or disable content packs.

Follow these steps:

1. Log in to the business unit that contains the content pack that you want to enable or disable.

2. Click Service Builder, Configuration.

The Service Builder configuration options appear.

3. In the left menu, click Content Packs.

The list of imported content packs appears.

Note: The Catalog system imports all objects as inactive (disabled).

4. Click the content pack that you want and enable.

The content pack details appear, including the overview and the list of objects in each category. The overview includes the ID, name, description, version, and other general information about the content pack.

5. Enable or disable objects in the list, as follows:

- Activate *all objects* in the content pack by clicking the Enable button for the entire content pack. This button appears on the Content Pack Details bar.

Important! Use this option with caution. If the content pack contains rules, action, or policies that perform redundant or conflicting tasks, unpredictable results can occur. Therefore, if you are not certain regarding the purpose or goal of the content pack, then enable each object individually.

- Conversely, deactivate *all objects* in the content pack by clicking the Disable button for the entire content pack

- Enable or disable individual objects within a category by clicking the Enable or Disable button for the object.

You can enable or disable objects in any or all of the following categories:

- Services

Enabling a service activates its Date Available setting: The service uses its Date Available setting to determine whether and when it is available to users.

- Service Option Groups

Enabling a service option group activates its Date Available setting: The service option group uses its Date Available setting to determine whether and when it is available to users..

Note: Enabling a service or service option group sets its status to System Object--Available (6). Similarly, disabling a service or service option group sets its status to System Object--Unavailable (7).

- Policies

Enabling a policy sets its status to Active. Disabling a policy sets its status to Inactive.

You can make only limited updates to imported policies that you have enabled. To make additional updates to such policies, copy and modify them.

- Rules

You enable or disable rules individually, without affecting the status of any other rules in the same event.

Note: Enabling or disabling a rule does not automatically enable or disable the actions in the rule. The actions remain in the original status.

- Actions

You enable or disable actions individually, without affecting the status of any other actions in the same rule. Similarly, enabling or disabling an action does not affect the status of the rule that contains the action.

Note: Enabling and disabling does not apply to the following objects: events, forms, reports, images, and CA Process Automation processes. You specified during the import whether to make CA Process Automation processes active or inactive.

6. Click Done when you are finished enabling and disabling objects in the content pack.
7. (Optional) Verify that the object is enabled (active) or disabled (inactive) by viewing its status. For example, select Services, folder-name, and open a service that you enabled. Verify that its status is System Object--Available. Also verify that its Date Available meets your requirements.

You have enabled or disabled objects in content pack. All objects that you enabled are available in the Catalog system.

Note: When you enable or disable objects in a content pack, your action does not affect any *copies* of those objects. You enable or disable each copy individually in a separate action.

Chapter 7: Content Configuration Form

This section contains the following topics:

[Overview of Content Configuration Form](#) (see page 91)

[Create the Content Configuration Form](#) (see page 92)

[Retrieve Values from Fields on Content Configuration Forms](#) (see page 94)

Overview of Content Configuration Form

You can optionally [create a content configuration form](#) (see page 92) to specify any custom configuration information required to use your content pack. These forms are typically not required but can be helpful, especially under the following circumstances:

- The imported objects require configuration before you can use them.
- The administrator who imports the content pack did not export it.
- You require custom values for variables in API plug-ins or CA Process Automation processes. Instead of hard-coding specific values, you can [retrieve values from fields on content configuration forms](#) (see page 94). Typically, you use this tactic when the values can change and cause the API plug-ins or CA Process Automation processes to fail, leading to system downtime. Examples include a server URL that can change, for example, because of a test-to-production move or a migration from a low-security to high-security environment.

Content configuration forms can be helpful when your imported content requires a custom configuration for one or more of the following:

- CA Process Automation processes and plug-ins that require configuration data
- A plug-in that needs access to an external data source (not the MDB), such as web service or database

An example is an Active Directory query that supplies CA EEM. The configuration form can list a *server name=field-name* field. The Active Directory query references this field in the form, rather than a hard-coded server name.

- Organization-specific requirements, such as user names and passwords that change both at regular intervals and intermittently as-needed.

Content configuration forms are specific to the business unit for which you create them. Parent business units have access to the forms of their child business units.

Administrators of each business unit can define their own configuration forms in the same way as they can define request forms. Additionally, the Service Builder, Configuration, Content Configuration page includes the Change Business Unit button. This button behaves the same way as on other Service Builder pages: it opens a dialog that lets you select another business unit that you are authorized to access. If you change business units, the list of configuration forms on the left pane of the page updates to display the forms of the current business unit.

Create the Content Configuration Form

To create a content configuration form, follow this process:

Note: For more details about creating forms using the Form Designer, see the *Administration Guide*.

1. Decide the purpose of the configuration form. Examples include specifying custom *parameter=value* expressions for API plug-ins or CA Process Automation processes.

Note: These custom expressions are *not* the same as the parameters on the Administration Configuration page, the Accounting Configuration page, or the Service Builder Configuration page. Moreover, these expressions are *not* the same as any other parameters on the CA Service Catalog GUI. Custom parameters can *complement* the GUI parameters, but they are not required to do so.

2. Determine the fields required on the form. Create fields that require user input to determine configuration data that the Catalog system saves and uses.

Examples include the following fields, which supply database parameters:

- Server name or URL
- User name
- Password
- Port number

Note: This form applies to your business unit *only*. Therefore, queries to the fields on the form from API plug-ins or CA Process Automation processes must specify the business unit.

3. Create the form in the Form Designer. Follow these guidelines:
 - For the Form attributes, specify a value of configuration for the Form Type attribute.
 - Be careful to create *unique* configuration forms, especially if you use multiple configuration packs. A unique configuration form has unique value for the `_id` attribute in the Form attributes. Verify that no other configuration form in your business unit has the same value for that attribute.

4. Open the form on the Service Builder, Configuration, Content Configuration page and specify the values you want in each field. Follow these guidelines:
 - As a best practice, specify default values that can help run the content pack successfully without the user changing any data. Doing so is helpful if the user creating or exporting the content pack is not familiar with it.
 - Optionally specify `_.bu` and `_.user` JSON objects as values. You *cannot* specify any other JSON objects as values.
5. Save the form.

Note: If you import configuration forms using content packs, the values for the form fields are not available until you save them on this page. This page is the Service Builder, Configuration, Content Configuration page that you opened previously.

Retrieve Values from Fields on Content Configuration Forms

At times, you require custom values for variables in API plug-ins or CA Process Automation processes. In such cases, instead of hard-coding specific values, you can save such values on the content configuration form. Typically, you use this tactic when the values can change and cause the API plug-ins or CA Process Automation processes to fail, leading to system downtime. Examples include a server URL that can change, for example, because of a test-to-production move or a migration from a low-security to high-security environment.

Important! The values on a content configuration form can have a maximum length of 4,000 characters for single-byte languages, for example, English. The values can have a maximum length of 2,000 characters for double-byte languages, for example, Chinese or Japanese. For example, a select box with a very large number of options can exceed this limit and cause errors.

Follow these steps:

1. (API plug-in) If you use a custom API plug-in, locate the `com.ca.usm.plugins.apis.PluginContext` object. In that object, use one of the following methods to retrieve values from fields on a content configuration form:

Object `getCatalogConfigValue(String configGroup, String tenantId, String configName)`;

Queries *one* field on the form. This method returns the value of the configuration parameter.

Specify values for the following parameters:

configName specifies the value of the `_id` attribute of the field on the form.

configGroup specifies the literal value "ca_cc_" followed by the value of the `_id` attribute of the form. An example is `ca_cc_form1`.

tenantId specifies the business unit ID, for example, `ca.com`.

Map<String, Object> `getCatalogConfigValues(String configGroup, String tenantId)`;

Queries *all* fields on the form. This method returns the map of key value pairs, where the keys are the values of the `_id` attributes of the fields on the form.

For `configGroup` and `tenantId`, the same values apply as for the previous method, `Object getCatalogConfigValue`.

2. (CA Process Automation) If you use a custom CA Process Automation process, link the process to one of the following methods in the CA Service Catalog web services.

You link the process and the method so that you can retrieve values from fields on a content configuration form:

```
public String getConfigurationValue(String sessionId, String configGroup, String tenantId, String configName)
```

```
public Map<String, Object> getConfigurationValues(String sessionId, String configGroup, String tenantId)
```

The parameter explanations are the same as for the methods in the previous step, except session ID.

session ID uniquely identifies the session. It is a required parameter that the client uses for the remaining web service calls.

Note: For more information about creating CA Process Automation processes and Start Request Forms, see the CA Process Automation documentation. For more information about web services, see the *Administration Guide* and the *Web Services API Documentation*.

You have retrieved values from the form fields.

Chapter 8: Configuring

This section contains the following topics:

- [Integrations](#) (see page 97)
- [Obtain Product License Keys](#) (see page 98)
- [Service Delivery Administrator](#) (see page 98)
- [Assign the Service Delivery Administrator Role to a User](#) (see page 99)
- [Change Your Password](#) (see page 100)
- [Verify that Browser Security Settings Permit Login](#) (see page 101)
- [How to Enhance Security](#) (see page 102)
- [Required Open Ports](#) (see page 103)
- [How to Enable External Authentication of Users](#) (see page 104)
- [How to Configure CA Service Catalog to Use Secure Socket Layer](#) (see page 106)
- [How to Verify Configuration Settings](#) (see page 117)
- [Inheritance of Configuration Settings Through the Business Unit Hierarchy](#) (see page 118)
- [Administration Configuration Options](#) (see page 119)
- [Accounting Configuration Options](#) (see page 138)
- [Set Service Builder Configuration Options](#) (see page 169)
- [Configuration of Web Services](#) (see page 186)
- [Single Location for Shared Files](#) (see page 186)
- [Advantages of 64-Bit Mode](#) (see page 189)
- [Configure Components to Run in 64-Bit or 32-Bit Mode](#) (see page 189)
- [Updates Made by the Ant Command](#) (see page 191)

Integrations

Some of the most important post-installation tasks focus on configuring the [integrations](#) (see page 23) between CA Service Catalog and other products, as follows:

- Importing, managing, and synchronizing the CA Service Catalog user database, using either the embedded solution CA EEM or an external directory, such as Microsoft Active Directory. This integration is required.
Important! If you use an external directory, configure CA EEM and CA Service Catalog to work with it.
- Authenticating users who log in to CA Service Catalog, using either CA EEM or CA SiteMinder.
- Integrating with CA Business Service Insight.
- Integrating with Reservation Manager.
- Integrating with CA Service Desk Manager, which includes CA CMDB.

- Setting up automated workflows to manage the requests for services that users make through CA Service Catalog, using either CA Process Automation (the preferred solution) or CA Workflow.
- Integrating with the asset management solution, CA APM. This integration is especially helpful when your organization tracks physical assets included in CA Service Catalog requests.
- Integrating with CA SRM.
- Integrating with CA MICS or CA JARS.

Note: For details to perform each of these tasks, see the *Integration Guide*.

Obtain Product License Keys

After you install CA Service Catalog or another CA product, you can use the product for 30 days. After that time, you must obtain a license key for each product that you intend to continue using.

To obtain license keys, access <http://ca.com/support>.

Note: You can also use this site to request assistance, to acquire additional licenses, and for instructions to apply license keys.

Service Delivery Administrator

Typically, the CA Service Catalog installation creates a user named "spadmin" and assigns it the Service Delivery administrator role. This user has complete control of the Catalog system. By default, the user name and the password are the same.

However, if CA EEM is already installed and configured to use an external directory (such as Microsoft Active Directory), then the installation *cannot* create this user. In this case, use the add-spadmin-user command utility to add the Service Delivery Administrator role to an existing user. Doing so enables this user to log in to CA Service Catalog using the Service Delivery Administrator role and to perform functions that require this role.

In certain cases, however, the installation cannot create this user. In such cases, [assign the Service Delivery Administrator role to another user](#) (see page 99).

You can also use this utility to assign the Service Delivery Administrator role to additional users. Having additional users with this role is optional but is beneficial if redundancy is important in your organization.

As a best practice and for increased security, we recommend that you log in to CA Service Catalog as the spadmin user and [change its password](#) (see page 100).

Assign the Service Delivery Administrator Role to a User

Typically, the installation program creates an administrative user named *spadmin* with the [Service Delivery Administrator](#) (see page 98) role. This user has complete control of the Catalog system. In [certain cases](#) (see page 98), however, the installation cannot create this user. In such cases, assign the Service Delivery Administrator role to another user. You can also assign the Service Delivery Administrator role to additional users. Doing so is optional but is beneficial if redundancy is important in your organization.

To assign the Service Delivery administrator role to a user

1. Open the CA Service Catalog command prompt by clicking Start, Programs, CA, Service Catalog, Service Catalog Command Prompt.
2. Enter the following command at the CA Service Catalog command prompt:

```
ant add-spadmin-user
```

Note: For a list of ant commands and their descriptions, enter `ant -p`.
3. Follow the prompts to add the spadmin administrator role to a specific user, using the following information:
 - If CA EEM *is* configured to use an external directory (such as Microsoft Active directory), specify an existing user name.
 - The command utility creates the user in the CA Service Catalog user database, if both of the following conditions exist:
 - CA EEM *is not* configured to use an external directory.
 - The user name that you specify is new.
 - The utility does *not* prompt you for the password of the new or updated user.
 - If CA EEM *is* configured to use an external directory, the password is defined and stored in the external directory.
 - The new password is the same as the user name, if both of the following conditions exist:
 - CA EEM *is not* configured to use an external directory.
 - The user name that you specify is new.
4. Cancel and rerun the `ant add-spadmin-user` command to correct any errors, if necessary.

5. Verify that the new or updated user can do the following:
 - Log in to CA Service Catalog
 - Update the password (if applicable)
 - Perform functions that require the Service Delivery Administrator role
6. Instruct the new user to change the password.

This action is a best practice and helps maintain security.

You have assigned the Service Delivery Administrator role to a user.

Change Your Password

You can change your password quickly and easily. You can change it at regular intervals to comply with the policies of your organization. In addition, you can also change it at any time, for various security-related reasons. Changing the password is especially recommended for the [user named spadmin](#) (see page 98) (the Service Delivery administrator).

To change your password

1. Log in to CA Service Catalog with your current user name and password.
2. Click Profile.

Your user profile appears.
3. Click the Change Password button at the top right of the page.

The Change User Password dialog appears.
4. Enter your old and new passwords in the fields provided.
5. Click OK.

You have changed your password.

Verify that Browser Security Settings Permit Login

This topic applies *only* if you are using Internet Explorer to access CA Service Catalog. Your browser security settings can prevent you from seeing the user name and password prompts when you attempt to log in to CA Service Catalog. Therefore, verify your browser security settings to help ensure that you can access CA Service Catalog.

Verify that security settings permit login

1. Open Internet Explorer on the computer you want to use for accessing CA Service Catalog.
2. Enter the URL to start CA Service Catalog in the browser address field, in the format `http://computer-name:port number/usm/`.

computer-name

Specifies the name of the computer that you want to log in to.

port number

Specifies the CA Service Catalog port number of that computer.

3. Verify that you see the CA Service Catalog login page, including the user name and password prompts.

If Yes, this verification procedure is complete, and you can skip the remaining steps.

If No, complete the remaining steps.

4. In Internet Explorer, open Internet Options, click Security, and do *one* of the following:
 - Change the security level for the Local Intranet to Medium-High or Medium
 - Add the login URL for CA Service Catalog to your Trusted sites
5. Close and reopen your browser.
6. Enter the URL to start CA Service Catalog in the browser address field. Verify that you see the CA Service Catalog login page with the user name and password prompts.

You have verified your browser security settings to help ensure that you can access CA Service Catalog.

How to Enhance Security

To enhance security in your CA Service Catalog implementation, *consider* making the following configuration changes:

- Disable the Apache JServ Protocol (AJP) port, port 8009 while [performing the initial setup](#) (see page 219), if you are *not* implementing [clustering](#) (see page 215).

To do so, edit the %USM_HOME%\view\conf\server.xml file and verify that the AJP tags are commented out.

- Reduce the timeout of CA Service Catalog user sessions. By default, sessions time out after 60 minutes of inactivity.

To do so, log in to CA Service Catalog, click Administration, Configuration, [User Default](#) (see page 132). Adjust the Session Timeout parameter at your discretion.

- Configure the CA EEM password policies to be more secure, if CA EEM is *not* configured to use an external directory.

Specifically, consider locking user accounts after three to five failed login attempts. To set this value, log in to CA EEM and click Configure, EEM Server, Password Policies.

- Update the list of roles that can run web services. By default, only the Certificate user and users with the service provider (SP) administrator role can run web services.

To change this list, log in to CA EEM with the Application set to Service Catalog. Click Manage Access Policies, Policies, Access Policies, USM_Resource. Edit the policy whose permissions you want to update, and add the resource named usm_webservice__all to that policy.

Note: For details about editing these policies, see your CA EEM documentation.

- Enable Secure Socket Layer (SSL) for web services so that passwords are not sent in plain text when you use the `login(String,String,String)` method. If SSL is not available, consider using the `loginToken(String)` method instead. This method takes an CA EEM artifact as a parameter and is encrypted.
- Install antivirus software on the filestore computer, if you are using a [filestore](#) (see page 187) (a single location for shared files). We strongly suggest that you do, to help ensure that any malicious files inadvertently uploaded using Home, Documents are quarantined and do not affect security.

- Harden CA Service Catalog computers.

Hardening is the process of securing a computer by removing or disabling components or access points, to render the computer less vulnerable to outside attacks. Hardening may include disabling all ports on a computer initially and afterwards manually enabling individual ports as needed. Other basic hardening steps include the following: Limit the number of users permitted access to a computer, strengthen password and access control, install intrusion-detection software, and close ports.

If you have hardened CA Service Catalog computers, [verify that the required ports are open](#) (see page 103) on these computers.

Other security-related instructions that apply to specific tasks or integrations are mentioned where applicable in the CA Service Catalog documentation.

Required Open Ports

CA Service Catalog requires the following ports for communication with products and components. If you have disabled these ports, for hardening purposes or for any other reasons, enable them.

Note: For instructions to enable ports, see your Windows documentation.

Product or Component	Default Port
Service View (includes access for CA Service Catalog and CA Service Accounting)	8080
CA Process Automation, CA Service Desk Manager, BusinessObjects Enterprise, other CA products that integrate with CA Service Catalog	8080
Visualizer port for CA Service Desk Manager	9080
CA Workflow	8090
SQL Server server	1433
Oracle server	1521
CA EEM	5250
IMQ port of CA EEM	7676

If you are using nondefault ports, verify that they are open.

You do not need to open the shutdown ports for the products and components listed.

If you plan to [implement clustering](#) (see page 215) for Service View, CA Workflow, or both, open all Apache JServ Protocol (AJP) and load balancing ports.

If you have implemented HTTPS, open all ports that are required for HTTPS to function properly.

How to Enable External Authentication of Users

By default, CA Service Catalog uses CA EEM to authenticate users. However, you can optionally configure CA Service Catalog to authenticate users with external applications such as CA SiteMinder, IBM Tivoli, and others. The process consists of the following tasks:

1. Install and implement the external authentication application, according to its documentation.

Note: If you are using CA SiteMinder as your external authentication application, see the *Integration Guide* for instructions to integrate CA Service Catalog and CA SiteMinder.

2. Do one of the following:
 - [Configure NTLM authentication on Windows](#) (see page 105), if applicable.
 - [Configure the single sign-on type setting](#) (see page 106) to match the external authentication application.
3. For reference, review the following examples to see how these applications typically send user authentication to CA Service Catalog. If applicable, adjust your settings to match these examples.
 - CA SiteMinder sends user identity information (authenticated user) with sm-user artifact name in the request header
 - IBM Tivoli sends user identity information with iv_user artifact name in the request header
 - Microsoft Internet Information Server (IIS) sends user identity information with request when configured for Windows NTLM
 - Apache sends user identity information with request when configured for Windows NTLM
 - For other external authentication applications, see their documentation

4. Test the configuration on both CA Service Catalog and the external authentication application.
5. Verify that CA Service Catalog successfully receives and processes the authenticated users that the external authentication application passes. If necessary, adjust the parameters on both systems as needed.

Configure NTLM Authentication on Windows

By configuring NTLM Authentication on Windows, you can enable single sign-on (also named single sign-in or single signin) for CA Service Catalog. Doing so means that once users log in to your domain, they can access CA Service Catalog without logging in to it. If you do not enable single sign-on, the login page is the first CA Service Catalog screen that users see. This topic explains how to modify the CA Service Catalog configuration to skip the login page.

If you are planning to use Service View [clustering](#) (see page 215) with NTLM authentication, skip this procedure. Instead, you set up NTLM authentication for each cluster.

Follow these steps:

1. Verify that your environment meets the following requirements:
 - You are using Windows domain authentication.
 - You have configured CA EEM to use Active Directory.
Note: For instructions to configure and use CA EEM, see the *Integration Guide*.
 - The CA EEM server has joined the Windows domain that you are configuring for single sign-on.
 - You are running a version of HTTP *higher* than 1.0. Windows NTLM authentication is supported with versions of HTTP higher than 1.0.
 - If both of the following conditions exist, you cannot use single sign-on using NTLM with HTTPS:
 - The client computer operating system is Windows Server.
 - The Internet Explorer Enhanced Security Configuration Windows Component is installed.

If you are using Windows Server, do one of the following to use single sign-on using NTLM:

 - Use HTTP instead of HTTPS.
 - Uninstall the Internet Explorer Enhanced Security Configuration Windows Component.
2. Click Administration, Configuration, Single Sign On Authentication.
The Single Sign On Authentication page appears.

3. Locate the property named Single Sign On Type and click its Modify icon (by default, a pencil).

The Edit Configuration dialog for this property appears.

4. Select the option named NTLM (NT LAN Manager) and click Update Configuration.

The dialog closes, and you return to the Sign On Authentication page.

You have configured NTLM Authentication on Windows.

Configure Single Sign-on Type Setting for External Authentication

Configuring the external authentication parameters is a required task to [enable external authentication of users](#) (see page 104) through an external application such as CA SiteMinder or IBM Tivoli. This topic applies if you use external authentication. In that case, verify that the Single Sign-on Type setting for external authentication is correct for your implementation.

Follow these steps:

1. Click Administration, Configuration, Single Sign On Authentication.

The Single Sign On Authentication page appears.

2. Locate the property named Single Sign On Type and click the Modify icon (a pencil icon by default).

The Edit Configuration dialog for this property appears.

3. Select the option named Artifact Based Single Sign-on and click Update Configuration.

The dialog closes, and you return to the Sign On Authentication page.

You have configured the Single Sign-on Type setting for external authentication.

How to Configure CA Service Catalog to Use Secure Socket Layer

You can optionally configure CA Service Catalog to use Secure Socket Layer (SSL). To do so, perform the following tasks. When you configure a product to use SSL, you change its communication method from HTTP to HTTPS.

1. Verify that you have a valid keystore containing a trusted certificate. If you have one for another product, you can reuse it for CA Service Catalog.
2. (Optional) [Create a keystore file](#) (see page 108). This procedure includes generating a certificate and a keystore for testing purposes, using the Java keytool command.

3. Use a single keystore for all integrated products, if possible. This approach is recommended.

However, if you have multiple keystores for different products and cannot use a single keystore for all of them, you can optionally [merge keystore files](#) (see page 109). This procedure includes merging the contents of the individual keystore files, resulting in one keystore containing all certificates.

4. [Configure Service View to Use Secure Socket Layer](#) (see page 110).
5. If you are integrating CA Service Catalog with CA Process Automation, do the following:
 - a. Configure CA Process Automation to use Secure Socket Layer
Note: For instructions, see your CA Process Automation documentation.
 - b. [Configure CA IT PAM to communicate with CA Service Catalog using Secure Socket Layer](#) (see page 114)
6. If you are integrating CA Service Catalog with CA Workflow, do the following:
 - a. [Configure CA Workflow to use Secure Socket Layer](#) (see page 111)
 - b. [Configure CA Workflow to communicate with CA Service Catalog using Secure Socket Layer \(SSL\)](#) (see page 113)
7. If you are integrating CA Service Catalog with BusinessObjects Enterprise, do the following:
 - a. Configure BusinessObjects Enterprise to use Secure Socket Layer
Note: CA Business Intelligence packages and delivers BusinessObjects Enterprise. Therefore, you use CA Business Intelligence to configure BusinessObjects Enterprise to use SSL; for instructions, see your CA Business Intelligence documentation.
 - b. [Configure BusinessObjects Enterprise to communicate with CA Service Catalog using Secure Socket Layer](#) (see page 115)
8. [Add self-signed certificates to the keystore](#) (see page 116), if applicable.

Create a Keystore File

A keystore file is required to enable SSL. Create a keystore file to enable SSL for CA Service Catalog if you do not have one already for another CA product that integrates with CA Service Catalog. You can use a keystore file for a single product or for multiple products. If you must create individual keystores for each product, you can optionally [merge your keystore files](#) (see page 109).

To create a keystore file

1. Open a command window on the Service View server.
2. Enter the following command to create a keystore file for CA Service Catalog:

```
keytool -genkey -alias alias_name -keyalg RSA -keystore "%USM_HOME%\keystore"
```

alias_name

Specifies the name of your keystore file for CA Service Catalog and possibly for other products.

3. Record this alias name for future reference.
4. Enter the password you want at the “Enter keystore password” prompt.
To make configuring Tomcat easier, you can use “changeit” as the password.
5. Record your password for future reference.
6. Enter your password at the prompt.

You have created the keystore file.

Merge Keystore Files

A keystore file is required to enable SSL. We recommend this approach, if possible: If you are using SSL for two or more products and have two or more keystore files, use a single keystore for all integrated products. However, if you have multiple keystores for different products and cannot use a single keystore for all of them, you can optionally do the following: Merge the contents of the individual keystore files, resulting in one keystore containing all certificates.

To merge keystore files

1. Copy all keystore files to the %USM_HOME% folder. These files include, for example, any keystore files for CA Process Automation, CA Workflow, CA CMDDB, CA Service Desk Manager, or other products that integrate with CA Service Catalog.
2. Find and record all required keystore files, keystore aliases, and keystore passwords for the products of interest.

For example, for CA Process Automation, at publication time, you can retrieve the c2okeystore password from KEYSTOREID property of the OasisConfig.properties file. A sample value follows:

```
KEYSTOREID=475ba811-62cd-4ec8-b757-cd7710de3fa8
```

Note: For further details, see the documentation for those products.

3. Restart Service View.
4. Enter the keytool command to merge the keystore of the first product, using the following command as a model:

```
keytool -importkeystore -srckeystore ".product1_keystore" -destkeystore
"%USM_HOME%\keystore" -srcalias product1_alias -destalias alias_name
-srckeypass "product1_password" -destkeypass "changeit"
.product1_keystore"
```

Specifies the name of keystore file (including the complete path name) for the product you are merging.

product1_alias

Specifies the keystore alias for the product you are merging.

product1_password

Specifies the keystore password for the product you are merging.

alias_name

Specifies the *alias_name* that you specified when you [created a keystore file](#) (see page 108) for CA Service Catalog.

For example, the following command merges the contents of the CA Process Automation keystore (.c20_keystore) into the CA Service Catalog keystore:

```
keytool -importkeystore -srckeystore "%ITPAM_HOME%\server\c20\config\c20keystore" -destkeystore "%USM_HOME%\keystore" -srcalias c20-j -destalias tomcat -srckeypass "475ba811-62cd-4ec8-b757-cd7710de3fa8" -destkeypass "changeit"
```

Another example follows. The following command merges the contents of the CA CMDB keystore (.cmdb_keystore) into the CA Service Catalog keystore:

```
keytool -importkeystore -srckeystore ".cmdb_keystore" -destkeystore "%USM_HOME%\keystore" -srcalias cmdb -destalias tomcat -srckeypass "changeit" -destkeypass "changeit"
```

5. Respond No when you are prompted to overwrite the source alias.
6. Repeat the previous two steps for each product whose keystores you are merging.
7. Verify if all the certificates that you want are in one keystore, using the following command:

```
keytool -list -keystore "%USM_HOME%\keystore"
```

This command lists the contents of the merged keystore.

You have merged keystore files.

Configure Service View to Use Secure Socket Layer

As part of configuring CA Service Catalog to use Secure Socket Layer (SSL), you configure Service View to use SSL.

To configure Service View to use SSL

1. [Edit the server.xml file to support SSL](#) (see page 112).
The file is updated to help support SSL for CA Service Catalog.
2. Open the %USM_HOME%\view\conf\viewService.conf file, using a text editor such as Notepad, and do the following:
 - a. Update the following line with the path name and file name of the keystore file:

```
wrapper.java.additional.number=Djavax.net.ssl.trustStore="%USM_HOME%\keystore"
```
 - b. Update the following line with the password of the keystore file:

```
wrapper.java.additional.number=Djavax.net.ssl.trustPass=changeit
```
 - c. Save and close the viewService.conf file.
3. On the CA Service Catalog GUI, select Administration, Configuration, Server Information.

The cursor moves to the Server Information section.

4. Complete the fields in this section as follows:
 For Host Name, specify the name of the host where Service View is installed.
 For Port Number, specify the port where HTTPS is configured.
 For Enable HTTPS, specify Yes.
5. Move to the CA Workflow configuration section and click Configure.
 The USM Workflow actors are updated to use HTTPS communication.
6. Restart Service View.
7. Log in to CA Service Catalog using the URL <https://hostname:port/usm/wpf> rather than URL <http://hostname:port/usm/wpf>.
 You see a trusted certificate prompt, which indicates that you are using HTTPS.
8. Optionally, disable HTTP access by commenting the section for the HTTP connector. To do so, add the "<!--" and "-->" comment markers to the first and last lines, as shown in the following example:

```
<!--
<Connector port="8080" enableLookups="true" redirectPort="8443"
    acceptCount="100" maxThreads="150" minSpareThreads="25" maxSpareThreads="75" debug="0"
    connectionTimeout="20000" disableUploadTimeout="true"
    useBodyEncodingForURI="false" URIEncoding="UTF-8" />
-->
```

You have configured Service View to use SSL.

Configure CA Workflow to Use Secure Socket Layer

As part of configuring CA Service Catalog to use Secure Socket Layer (SSL), you typically configure CA Workflow to use SSL.

To configure CA Workflow to use SSL

1. [Edit the server.xml file](#) (see page 112).
 The file is updated to help support SSL for CA Workflow.
2. Edit the %USM_HOME%\fulfillment\conf\FulfillmentService.conf file, using a text editor such as Notepad. Do the following:
 - a. Update the following line with the path name and file name of the keystore file:

```
wrapper.java.additional.number=Djavax.net.ssl.trustStore=%USM_HOME%.keystore"
```
 - b. Update the following line with the password of the keystore file:

```
wrapper.java.additional.number=Djavax.net.ssl.trustPass=changeit
```
 - c. Save and close the FulfillmentService.conf file.

3. Restart Service Fulfillment and Service View.
4. Start the CA Workflow IDE from the CA Service Catalog CA Workflow link.
You see a trusted certificate prompt, which indicates you are using HTTPS.

You have configured CA Workflow to use SSL.

Edit the Server.xml File to Support SSL

As part of [configuring Service View](#) (see page 110) or [configuring CA Workflow](#) (see page 111) to use Secure Socket Layer (SSL), you edit the server.xml file to support SSL.

Follow these steps:

1. Open the server.xml file using a text editor such as Notepad, as follows:
 - For Service View, open the %USM_HOME%\view\conf\server.xml file.
 - For CA Workflow, open the %USM_HOME%\fulfillment\conf\server.xml file.
2. Search for the following section and enable the commented section by removing "<!--" and "-->" from the first and last lines, as shown in the following example:

```
<!-- <Connector port="8444" maxHttpHeaderSize="8192"
      maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
      enableLookups="false" disableUploadTimeout="true"
      acceptCount="100" scheme="https" secure="true" keyAlias="alias_name"
      clientAuth="false" sslProtocol="TLS" keystoreFile="C:\Program Files\CA\Service
      Delivery\keystore"/> -->
```
3. Update the default port (8444) to another secure socket layer port, if necessary.
Note: If you update the port number in this step, also update the port number on the GUI by clicking Administration, Configuration, Options, CA Workflow, Port Number.
4. Verify whether either or both of the following conditions exist:
 - You are using an existing keystore.
 - You have changed either the CA Service Catalog installation path or generated keystore name.
5. Do the following in the lines of the file shown earlier, if either or both of the conditions in the previous step exist:
 - Update the keystoreFile parameter with the correct path and file name, typically %USM_HOME%\keystore.
 - Update the keyAlias parameter with the *alias_name* that you specified when you [created a keystore file](#) (see page 108) for CA Service Catalog.

6. Save and close the server.xml file.

You have edited the server.xml file. You can continue [configuring Service View](#) (see page 110) or [configuring CA Workflow](#) (see page 111) to use Secure Socket Layer (SSL).

Configure CA Workflow to Communicate with CA Service Catalog Using Secure Socket Layer

As part of configuring CA Service Catalog to use Secure Socket Layer (SSL), you configure CA Workflow to communicate with CA Service Catalog using SSL.

To configure CA Workflow to communicate with CA Service Catalog using Secure Socket Layer

1. On the CA Service Catalog GUI, select Administration, Configuration, CA Workflow.
The cursor moves to the CA Workflow section.
2. Complete the fields in that section as follows:
For Host Name, specify the name of the host where CA Workflow is installed.
For Port Number, specify the CA Workflow port where HTTPS is configured.
For Enable HTTPS, specify Yes.
3. Recycle Service View.
4. Click Test.
The connection is tested, using the new values you specified.
If the connection fails, try using a different value.
5. Click Configure.
The CA Workflow actors are updated with the new values that you specified.
6. Recycle Service Fulfillment.

You have configured CA Workflow to communicate with CA Service Catalog using SSL.

Configure CA IT PAM to Communicate with CA Service Catalog Using Secure Socket Layer

As part of configuring CA Service Catalog to use Secure Socket Layer (SSL), you configure CA Process Automation to communicate with CA Service Catalog using SSL.

To configure CA Process Automation to communicate with CA Service Catalog using Secure Socket Layer

1. On the CA Service Catalog GUI, select Administration, Configuration, CA IT Process Automation Manager.

The cursor moves to the CA IT Process Automation Manager section.

2. Complete the fields in this section as follows:

For Host Name, specify the name of the host where CA Process Automation is installed.

For Port Number, specify the CA Process Automation port where HTTPS is configured.

For Enable HTTPS, specify Yes.

3. Recycle Service View.
4. Click Test.

The connection is tested, using the new values you specified.

If the connection fails, try using a different value.

5. Click Configure.

The CA Process Automation configuration details are updated with the new values that you specified.

Configure BusinessObjects Enterprise to Communicate with CA Service Catalog Using Secure Socket Layer

As part of configuring CA Service Catalog to use Secure Socket Layer (SSL), you configure BusinessObjects Enterprise to communicate with CA Service Catalog using SSL.

To configure BusinessObjects Enterprise to communicate with CA Service Catalog using Secure Socket Layer

1. On the CA Service Catalog GUI, select Administration, Configuration, CA Business Intelligence.

The cursor moves to the CA Business Intelligence section.

Note: CA Business Intelligence packages and delivers BusinessObjects Enterprise; therefore, you use these CA Business Intelligence parameters to configure the integration of CA Service Catalog with BusinessObjects Enterprise. For details about these parameters and about the relationship between CA Business Intelligence and BusinessObjects Enterprise, see the *Integration Guide*.

2. Complete the fields in this section as follows:

For Host Name, specify the computer name on which the InfoView component of BusinessObjects Enterprise is hosted.

For Port Number, specify the port number on which InfoView is running.

For Enable HTTPS, specify Yes.

3. Recycle Service View.
4. Click Launch.
5. The connection is tested, using the new values you specified. If the connection fails, try using a different value.

The BusinessObjects Enterprise configuration details are updated with the new values that you specified.

Add Self-Signed Certificates to the Keystore

When you use self-signed certificates for any computer that connects directly to CA Service Catalog or that CA Service Catalog connects to, add these certificates to the keystore. For example, suppose you are using [clustering](#) (see page 215) with [load balancing](#) (see page 236) for CA Service Catalog. In that case, if you are using a self-signed certificate for the load balancing computer, add them the keystore.

Note: If you are using trusted certificates, for these computers you do not need to add them the keystore.

To add self-signed certificates to the keystore, follow these steps:

1. Verify the computer to be trusted, that is, the computer that has direct connection with CA Service Catalog.

For example, suppose you integrate CA Service Catalog with CA Service Desk Manager through a load balancing computer. In that case, CA Service Catalog connects directly to the load balancer (not CA Service Desk Manager). Therefore, the computer to be trusted is the load balancer (not the CA Service Desk Manager computer).

2. Go to a Service View computer and download the DER encoded binary X.509 file (the certificate) for the computer to be trusted.

For example, use your web browser to visit the computer and obtain the certificate.

Note: For assistance to use your web browser for this purpose, see its documentation.

3. Open the CA Service Catalog command prompt and enter the following command:

```
keytool -importcert -alias aliasname -file pathname-to-certificate -keystore %USM_HOME%\keystore
```

pathname-to-certificate-file

Specifies the complete path name to the certificate file that you downloaded in the previous step.

You are prompted to enter a password.

4. Do one of the following:
 - Enter changeit as the keystore password.
 - Enter a different keystore password.

The password you enter is saved.

5. Complete this step if you entered a different password than *changeit* in the previous step. Otherwise, skip this step.
 - a. Open the `viewService.conf` file for editing.
 - b. Find the line that contains the following phrase:

```
-Djavax.net.ssl.trustPass=keystore-password
```
 - c. Update the `keystore-password` to match the new password that you specified in the previous step.

The `viewService.conf` file is updated with the new password.

6. Remain at this Service View computer. Repeat the previous steps for every computer to be trusted that has self-signed certificates.

As you repeat these steps, the keystore file is updated with the new self-signed certificates from each applicable computer to be trusted.

7. Do the following on of every other Service View computer:
 - a. Update the `viewService.conf` file to use a password other than *changeit*, if applicable, as explained in Step 5.
 - b. Copy the updated `.keystore` file from this Service View computer to all the remaining Service View computers.

You have you added self-signed certificates to the keystore.

How to Verify Configuration Settings

After the CA Service Catalog installation is complete, verify the configuration settings. Doing so helps ensure that the product functions according to the needs of your organization.

Verify the settings by group, as follows:

- [Administration configuration](#) (see page 119)
These include [integration-specific options](#) (see page 121)
- [Accounting configuration](#) (see page 138)
- [Service Builder configuration](#) (see page 169)
- [Web services configuration](#) (see page 186)
- [Location of shared files \(filestore\)](#) (see page 187)
- [Configuration of 64-bit or 32-bit mode](#) (see page 189)

Inheritance of Configuration Settings Through the Business Unit Hierarchy

The following rules govern the relationship between parent and child business units (children), including the inheritance of configuration settings:

- The child business units directly under the top-level business unit (the service provider) are named super business units. Super business units *always* inherit their configuration settings from the service provider business unit.
- A super business unit can have children if its configuration parameter named Contains Sub Units is enabled. Conversely, if this setting is disabled, the business unit cannot have children.

Note: After you have created the business unit, you *cannot* change its Contains Sub Units setting.

- Similarly, if the Contains Sub Units parameter of the super business unit is enabled, you *can* edit the configuration settings of the super business unit. Conversely, if this parameter is disabled, you *cannot* edit its configuration settings.
- If you edit the configuration settings of a super business unit, your changes do *not* apply to the super business unit itself. Instead, your changes apply to its children. A child "inherits" its configuration settings from its parent.
- You can optionally create unlimited levels of children, grandchildren, and so forth under super business units. For each business unit under the super business unit, the same parent-child relationship illustrated earlier applies, as follows:
 - If the Contains Sub Units setting of the business unit is enabled, you can edit its configuration settings. Your configuration changes do *not* apply to the business unit itself but instead apply to its children.
 - Conversely, if the Contains Sub Units setting of the business unit is disabled, you cannot edit its configuration settings.

Thus, the following summary applies to all business units except for the service provider:

- A business unit always inherits its configuration settings from its parent.
- You can edit the configuration settings of a business unit *only* if its Contains Sub Units setting is enabled. Your changes apply *only* to its children.

Note: For more information about business units, see the *Administration Guide*.

Administration Configuration Options

You can view and set administration configuration options that apply to all installed CA Service Catalog components.

To update administration configuration options, log in with the Service Delivery Administrator role. Updates to these options apply to the *entire* system. You *cannot* specify different administration configuration options for different business units.

Using the administration configuration options, you can do the following:

- [Set the values of the options](#) (see page 119)
- [Manage fiscal periods](#) (see page 135)
- [View product licenses](#) (see page 137)

Important! With one exception, CA Service Catalog sends emails in HTML format *only*. Therefore, to receive legible emails from CA Service Catalog, recipients must configure their email software, such as Microsoft Outlook, to accept emails in HTML format. Otherwise, emails from CA Service Catalog display indecipherable messages ("junk" characters) when opened. To help ensure that their end users can receive intelligible emails from CA Service Catalog, administrators *must* inform their end users of this requirement. If necessary, administrators *must* help them configure their email settings. The one exception to this HTML-only rule is *invoice history*. You can choose to view and email invoice history in HTML, CSV, or XML format. The HTML-only rule applies to all other invoice-related areas of CA Service Catalog, including invoice generation.

Set Administration Configuration Options

To meet the requirements of your organization, you may need to customize several administration configuration options, including those for integrations, portals, request SLAs, authentication, and others

To set administration configuration options

1. Log in as a user with the Service Delivery Administrator role.
2. Click Administration, Configuration.

The Administration Configuration page appears. On the left, in the Menu under the main menu, Options is selected. On the right, links appear for each category (subset) of the administration configuration options.

3. Click the link for the category of options that you want to update, one of the following:
 - [Integration-specific options](#) (see page 121)
 - [CA Workflow configuration](#) (see page 121)
 - [Event Manager](#) (see page 123)
 - Filestore information, for [setting up a filestore](#) (see page 187) (a single location for shared files)
 - [Mail server configuration](#) (see page 124)
 - [Portal](#) (see page 126)
 - [Request SLA Processor](#) (see page 127)
 - [Rule Engine](#) (see page 127)
 - [Server information](#) (see page 128)
 - [Single sign on authentication](#) (see page 129)
 - [System information](#) (see page 131)
 - [User default](#) (see page 132)

The options appear for the category that you clicked.

4. View the options for the category, and click the Modify icon (by default, a pencil) for the option that you want to update.

The Edit Configuration dialog appears.

5. Update the setting as required and click Update Configuration to save your update.
6. Repeat the previous steps for each administration configuration option that you want to update.

You have set the administration configuration options. These settings apply to the children of the business unit that you updated, according to the [inheritance of configuration settings through the business unit hierarchy](#) (see page 118).

Integration-Specific Options

If you are integrating CA Service Catalog with any of the following products, set the related configuration parameters. Doing so helps ensure that CA Service Catalog and the integrating product work together correctly. This task is part of [setting the administration configuration options](#) (see page 119).

- CA APM
- CA Business Intelligence

Note: CA Business Intelligence packages and delivers BusinessObjects Enterprise; therefore, you use these CA Business Intelligence parameters to configure the integration of CA Service Catalog with BusinessObjects Enterprise.
- CA CMDB
- CA CMDB Visualizer
- CA Process Automation
- CA Business Service Insight
- CA Service Desk Manager
- Reservation Manager
- **Note:** For information about setting these parameters and for related instructions to configure the integrations between CA Service Catalog and the following products, see the *Integration Guide*.

If you are using CA Workflow, set these configuration parameters to help ensure that CA Workflow and CA Service Catalog work together correctly. This task is part of [setting the administration configuration options](#) (see page 119).

To set the CA Workflow configuration parameters

1. Select Administration, Configuration, CA Workflow and specify values for the following parameters:

Enable HTTPS

Defines whether CA Service Catalog uses HTTPS when communicating with CA Workflow.

Default: No

Host Name

Displays the host name on which CA Workflow is installed. Update this setting if necessary.

Default: The host name on which this CA Workflow was installed.

Port Number

Specifies the port number used to communicate with CA Workflow.

Default: The value specified when CA Workflow was installed.

Retry Count

Specifies the number of times to try again to complete a failed CA Workflow action.

Default: 10

Retry Interval

Specifies the number of seconds between attempts to complete a failed CA Workflow action.

Default: 300

2. Recycle the CA Service View service.
3. Recycle the CA Service Fulfillment service.
4. Click Test to verify these parameters.
5. Click the Configure button to update the CA Workflow actors, if required. This action is required if you update any parameters in the Server Information section or the Service Desk section of the Administration Configuration parameters.

6. Verify whether *both* of the following conditions exist:
 - You are integrating CA Service Catalog with CA Service Desk Manager.
 - The related CA Service Catalog process definitions and actors are loaded in the CA Workflow implementation for CA Service Desk Manager.
7. If *both* of the conditions in the previous step exist, perform this step. Otherwise, skip this step.
 - a. Do the following, if any Server Information settings for CA Service Catalog have changed: Reimport the USM_RequestService web service actor loaded in the CA Service Desk Manager CA Workflow implementation with the new Server information. To do so, do the following, sequentially:
 - Export the actor in the CA Workflow IDE.
 - Change the wsdl_url to the new Server URL.
 - Reimport the actor into the CA Workflow IDE.
 - b. Update the USM_HW_Fulfillment_SD_r12 and USM_SW_Fulfillment_SD_R12 process definitions in the CA Workflow IDE. In each of these process definitions, select the Initialize Values function and set the USM_URL to the new Server URL.
 - c. Save the changes to these process definitions.
8. Recycle the CA Service Fulfillment service again.

Note: You can optionally click Launch to start the CA Workflow Process Manager.

Event Manager

As part of [setting the administration configuration options](#) (see page 119), you configure the following parameters for the Event Manager. The Event Manager processes events. An event occurs when one or more conditions specified in a rule are met.

Note: For information about events, rules, and actions, see the *Administration Guide*.

Email From

Sends an email *from* this address if the Event Manager has a problem.

Default: spadmin@*serviceprovider*, where “*serviceprovider*” is the root business unit specified during installation.

Email To

Sends an email *to* this address if the Event Manager has a problem.

Default: spadmin@*serviceprovider*, where *serviceprovider* is the root business unit specified during installation.

Audit Trail Level

Indicates the level of detail logged in the audit trail tables. Typically, system performance decreases as the level of log detail increases. Conversely, system performance typically increases as the level of log detail decreases.

Select one of the following options:

No Audit Trail

Stores no information about the event in the database.

Only Object ID

Stores the event information, including the object ID, in the `usm_system_change` table. This option stores only minimal information.

Include Attributes

Stores the event information, including the object ID, in the `usm_system_change` table. This option stores detailed old and new values for the object attributes in the `usm_system_change_detail` table.

Include Multiple Attributes

Stores the event information, including the object ID, in the `usm_system_change` table. This option stores detailed old and new values for the object attributes in the `usm_system_change_detail` table. If any attributes have multiple values, the old and new values are stored in the `usm_system_change_detail_ext` table.

Default: Include Attributes.

Mail Server

Important! Any mail-related settings in custom rule actions override these mail server parameters. For information about events, rules, and actions, see the *Administration Guide*.

As part of [setting the administration configuration options](#) (see page 119), you configure the following parameters for the mail server. The mail server sends automated messages from CA Service Catalog.

From Address

Specifies the address that emails are sent from.

Host Name

Specifies the host name of the mail server.

Port Number

Specifies the port number on the mail server that listens for incoming calls from CA Service Catalog.

User ID

Specifies the user ID for accessing the mail server.

User Password

Specifies the password for accessing the mail server.

Note: After you finish specifying these parameters, click the Test button to verify the connection between CA Service Catalog and the mail server. If the test fails, review the view.log file in the %USM_HOME%\logs folder.

These settings apply to the children of the business unit that you updated, according to the [inheritance of configuration settings through the business unit hierarchy](#) (see page 118).

Portal

As part of [setting the administration configuration options](#) (see page 119), you configure the following parameters for the Portal. The Portal settings specify how the dashboard library and document entries are made available.

Note: You can specify a value of No for any parameter that you do not need.

Allow New Document Domain Namespaces

Specifies whether business units can have their own document name spaces.

If this parameter is set to Yes, the Add A New Business Unit page contains the "Create Document Namespaces" check box.

The following is true if a business unit has its own document namespace: You can segregate documents in separate business units so that only users in that business unit have access to the document.

Default: Yes

Allow New Library Namespaces

Specifies whether business units can have their own library name spaces.

If this parameter is set to Yes, the Add A New Business Unit page contains the "Create Dashboard Namespaces" check box.

The following is true if a business unit has its own library namespace: You can segregate dashboard library content so that only users in that business unit have access to the library content when they add a dashboard.

Default: Yes

Show Resource Tree

Specifies whether the Resource Explorer appears in the dashboard library tree.

If this parameter is set to Yes, the Resource Explorer appears in the dashboard library tree. This option applies *only* if CA Service Catalog is integrated with CA Business Service Insight.

Default: Yes

Request SLA Processor

As part of [setting the administration configuration options](#) (see page 119), you configure the following parameters for the request SLA processor. These settings specify how the Catalog system processes request SLAs.

Note: For information about setting up request SLA processing, see the *Administration Guide*.

Maximum Delay for Request SLA Alerts

Specifies how frequently the request SLA processor checks for SLA warnings or violations. This setting applies to all SLA instances managed by a Service View computer.

To minimize possible delays in SLA processing time when a Service View clustered computer fails, configure the Maximum Delay for Request SLA Alerts setting. The smaller the value you set, the greater the frequency with which the request SLA processor checks the SLA clock for warning and violation times.

Therefore, set a smaller interval, such as one hour, to receive SLA warnings and violations quickly. Otherwise, set a larger interval, for example, one day, to receive them when the failed clustered computer is restored.

Rule Engine

As part of [setting the administration configuration options](#) (see page 119), you configure the following parameters for the Rule Engine. Administrators use rules to define actions to take when a specific event occurs. These actions can be running scripts or Java programs, sending emails, and so forth. The rule engine manages the execution of the actions.

Note: For information about events, rules, and actions, see the *Administration Guide*.

Action Default Timeout (in seconds)

Specifies the default timeout value in seconds for rule actions.

Default: 300

Server Information

As part of [setting the administration configuration options](#) (see page 119), you configure the following parameters for the Service View server. These settings apply *only* when you configure Service View for use with HTTPS or for use as a load balancer in clustering. Otherwise, Service View is configured automatically and the following parameters do *not* apply.

Important! If you update any parameters in the Server Information section, click **Configure** in the Workflow Configuration Parameters section. This action updates the CA Workflow actors!

Enable HTTPS

Defines whether CA Service Catalog uses HTTPS when communicating with this Service View computer.

Default: No

Host Name

Displays the host name of this Service View or load balancer computer.

Port Number

Specifies the port number used to communicate with this Service View or load balancer computer.

Important! If you use clustering, replace the host name and port number in the Server Information section with the load balancer host name and port number!

Single Sign On Authentication

As part of [setting the administration configuration options](#) (see page 119), you configure the following single sign-on authentication parameters. Give special care to the parameters for configuring CA Service Catalog to use external applications to authenticate CA Service Catalog users.

Allow Login with GET

When this configuration value is set to Yes, users can log in using an HTTP GET request.

When this configuration value is set to No, users *cannot* log in using an HTTP GET request.

Note: This parameter is not related to external authentication. Instead, it is used for backward compatibility of authentication-related features.

External Authentication Parameters

The external authentication parameters follow. To [enable external authentication of users](#) (see page 104), configure these parameter values to match the external application that you are using.

Artifact Name

Specifies the name of the cookie, header, or request parameter that contains the authenticated user ID. This name varies according to the external authentication system and your site-specific implementation.

The default value is sm-user.

For example, if you are using CA SiteMinder, select Header as the authentication type and sm-user as the artifact name. With this configuration, CA Service Catalog checks the header named sm-user whose value is the userid.

When the Artifact Type is request, the artifact name is ignored.

Artifact Type

Specifies the mechanism that the external application uses to send the authenticated user ID to CA Service Catalog, as follows:

- Cookie: Cookie in the request
- Header: Header in the request
- Parameter: request parameter
- Request: request user

Bypass Nodes

Specifies the GUI nodes that you want the authentication check to skip. These GUI nodes typically do not require the user to log in.

Examples include the following: `icguinode.login`, `icguinode.logout`, `iclaunchpad.launch`, `icguinode.changepwdlockout`, and `icguinode.lockout`.

Login Page

Specifies the page that displays to the user when either the artifact type is set incorrectly or CA Service Catalog does not find an authenticated user.

An example is `wpf?Node=icguinode.login`.

Single Sign-on Type

Specifies *one* of the following options:

- Disabled: Specifies that CA Service Catalog does *not* use single sign-on.
- Artifact Based Single Sign-on: Configures CA Service Catalog to use single sign-on based on the artifacts specified on this page.
- NTLM (NT LAN Manager): Configures CA Service Catalog to use single sign-on based on Windows NT authentication.

System Information

As part of [setting the administration configuration options](#) (see page 119), you configure the following settings related to common multi-tenant administration for CA Service Catalog business units:

Important! These settings apply *only* if you are *both* integrating CA Service Catalog with CA Service Desk Manager r12.5 *and* using common multi-tenant administration of CA Service Catalog business units. For information about setting up common multi-tenant administration, see the *Administration Guide*.

Terms Of Usage Prompt Enabled

After configuring CA Service Catalog to use common multi-tenant administration, optionally specify Yes for this setting. Doing so configures common tenants in CA Service Catalog to implement the terms of use (if any) that are created and maintained in CA Service Desk Manager. The specific effect on users attempting to log in to CA Service Catalog depends on the terms of use settings specified in CA Service Desk Manager.

The following is true when this setting is Yes: If users attempting to log in to CA Service Catalog receive the terms of use prompt but do not accept it, they cannot access CA Service Catalog.

The following is true when this setting is No: Users attempting to log in to CA Service Catalog are not prompted with terms of use, regardless of the terms of use settings specified in CA Service Desk Manager.

Note: For details about configuring terms of use in CA Service Desk Manager, see the CA Service Desk Manager documentation.

Common Multi-Tenant Administration Enabled

Specifies whether you manage CA Service Catalog business units with the common multi-tenant administration framework supplied through CA Service Desk Manager.

When this option is set to No, you manage CA Service Catalog business units directly through CA Service Catalog, and these business units are not synchronized with CA Service Desk Manager.

When this option is set to Yes, you cannot manage CA Service Catalog business units directly through CA Service Catalog, except for CA Service Catalog-specific attributes. Instead, you use the tenant administration tool of CA Service Desk Manager to manage all business units of CA Service Catalog and CA Service Desk Manager) and their common attributes.

You cannot set this option to Yes unless the Common Multi-Tenancy Model option is set to Yes.

Common Tenant Data Synchronized (read-only)

Specifies whether the CA Service Catalog tenant (business unit) structure is synchronized with the tenant structure of CA Service Desk Manager.

CA Service Catalog sets this option to Yes when all of the following conditions are met:

- CA Service Desk Manager is installed.
- The common multi-tenancy merge utility has run successfully.
- Since the utility was last run, no business unit has been created, deleted, or had a change in a common attribute through CA Service Catalog directly.

Conversely, CA Service Catalog sets this option to No when one or more of the following conditions exist:

- The common multi-tenancy merge utility has not run successfully.
- Since the utility was last run, one or more business units have been created, deleted, or had a change in a common attribute through CA Service Catalog directly.

User Default

As part of [setting the administration configuration options](#) (see page 119), you configure the following settings related to users, roles, searches, and sessions:

CA EEM Max Search Size

Defines the maximum number of users queried during searches in CA EEM. When you search for users in CA EEM, the number of users queried during the search does not exceed the number specified in this parameter.

Access Control: Allow Request Auto-Delegation via User Management

Defines which user roles are able to view and set auto-delegation for other users. Typically, administrator roles use this ability to set auto-delegation for users who are unable to set it for themselves. Examples of such employees include the following:

- Users who suddenly became unavailable due to emergency
- Users who left for a long absence without setting their own auto-delegation
- Users whose roles have no rights to set their own auto-delegation

Note: The next parameter, Access Control: Allow Auto-Delegation via User Profile, specifies whether employees can set their own auto-delegation.

The default value is the Service Delivery Administrator user role.

Access Control: Allow Request Auto-Delegation via User Profile

Defines which user roles have the Request Auto-Delegation setting appear on their User Profile window. Users with these roles can view and optionally configure this setting for themselves.

The default value is all user roles, so that all users can change at minimum their own auto-delegation settings.

User Default Role

Defines the default business-unit role assigned to a user when an administrator creates or edits the user.

If both of the following are true, the Catalog system assigns the default role to the user logging in:

- The user has an MDB record created by another product.
- That MDB record has never been edited through CA Service Catalog.

A change of this setting requires a restart of the Service View service to take effect.

The default value of this setting depends on the products installed:

- If CA Service Catalog is installed, the default value for this setting is Catalog User.
- If only CA Service Accounting is installed, the default value for this setting is End User.

User Search Scope

Defines how the scope of the “search user” functionality works for the Catalog User and End User roles. “Search user” functionality for these roles is available in the following areas:

- When emailing a request, users can populate the To, CC, and BCC fields by searching from a list of users or accounts.
- When editing the cart or a request, if the logged in user can create requests for other users or accounts (proxy requests), the following is true: The user can override the Requested For value by choosing from a list of users or accounts.

Note: The scope of “search account” functionality for Catalog End Users and End Users includes *only* accounts in the same business unit as the logged in user. This scope does *not* include child business units.

Select one of the following options:

- Enterprise - All users who have a User ID specified without regard to the role of the user. This setting is suitable for enterprise customers where business units represent departments in one company.

The scope of the “search user” functionality works as follows:

- A user who can change the Requested For user for a cart or a request can select from all users.

When a request is emailed, the list of users includes all users.

- Business Unit - All users who have a user ID and a role in the business unit of the logged in user. This setting is suitable for customers whose business units represent separate companies or departments within those companies.

The scope of the “search user” functionality works as follows:

- A user who can change the Requested For user for a cart or a request can select from users who have a role in the same business unit as the logged in user.
- When a request is emailed, the list of users includes only users who have a role in the same business unit as the logged in user.

Default: Enterprise

Session Timeout

Defines the number of minutes of inactivity after which users are logged out.

How to Manage Fiscal Periods

By default, you create monthly fiscal periods for the current year, based on your installation date. You also use fiscal periods to view Data Mediation aggregations and to manage budgeting and planning.

Note: You cannot create different fiscal periods for different business units. *Only one* set of fiscal periods applies to all business units.

To manage the fiscal periods for your CA Service Accounting implementation, do the following.

- [View the fiscal periods](#) (see page 135)
- [Add a fiscal period](#) (see page 136)
- [Edit a fiscal period](#) (see page 136)
- [Delete a fiscal period](#) (see page 137)

View Fiscal Periods

View fiscal periods to see which periods exist and to help you decide which periods to add, update, or delete.

To view fiscals period

1. Click Administration, Configuration.
The Administration Configuration page appears.
2. Click Fiscal Periods Under the Menu options on the middle left portion of the page, under the main menu.
The Budget and Planning: Fiscal Periods page for your business unit appears.

You have viewed the fiscal period.

Add a Fiscal Period

You add fiscal periods regularly according the fiscal schedule of your organization.

To add a fiscal period

1. Click Administration, Configuration.
The Administration Configuration page appears.
2. Click Fiscal Periods Under the Menu options on the middle left portion of the screen, under the main menu.
The Budget and Planning: Fiscal Periods page for your business unit appears.

3. Click the Add button.

The Fiscal Period Definition window opens.

4. Enter the following fields and click OK:

Name

Specifies the fiscal period name; for example, January or Q1.

Year

Specifies the fiscal period year; for example, 2012.

Start Date

Specifies the date the fiscal period starts.

End Date

Specifies the date the fiscal period ends.

Period

Select from the following list: Monthly, Quarterly, or Yearly.

Note: Fiscal periods of the same type cannot overlap dates.

You have added the fiscal period.

Edit a Fiscal Period

Edit fiscal periods when your organization requires you to do so, for example, to correct an earlier mistake.

To edit a fiscal period

1. Click Administration, Configuration.

The Administration Configuration page appears.

2. Click Fiscal Periods Under the Menu options on the middle left portion of the page, under the main menu.

The Budget and Planning: Fiscal Periods page for your business unit appears.

3. Click the name of the fiscal period that you want to edit.

The Fiscal Period Definition window opens.

4. Edit the same fields as when you [add a fiscal period](#) (see page 135).

5. Click Update Fiscal Period.

The system saves your changes.

You have edited the fiscal period.

Delete a Fiscal Period

Delete fiscal periods when your organization requires you to do so, for example, when they are being replaced.

To delete a fiscal period

1. Click Administration, Configuration.
The Administration Configuration page appears.
2. Click Fiscal Periods Under the Menu options on the middle left portion of the page, under the main menu.
The Budget and Planning: Fiscal Periods page for your business unit appears.
3. Select the select the name of each fiscal period that you want to delete.
4. Click the Delete button next to the “Select and” marker.
The fiscal period is deleted.

Verify the Product License

Verifying the product license is an important part of complying with ethical business practices, contractual agreements, and legal requirements.

To verify the product license

1. Click Administration, Configuration.
The Administration Configuration page appears. On the left, in the Menu under the main menu, Options is selected. On the right, links appear for each category (subset) of the administration configuration options.
2. Click Product License in the Menu on the left under the main menu.
The Product License Info page appears.
3. View the license Information, including the following:
 - Details about the license for each installed CA Service Catalog product or component
 - CA Service Catalog alerts related to licensing
 - Information about contacting CA for assistance with licensing

4. Click View License Alerts to check any alerts related to licensing.

The Alert Messages window opens.

Note: License alerts can occur when a CA Service Catalog license is about to expire. For details about system alerts, see the *Administration Guide*.

5. Contact your licensing officer or CA if any alerts appear.

You have verified the product license.

Accounting Configuration Options

You can view and set the accounting configuration options that apply to all installed CA Service Catalog components. These settings cover accounting profiles, billing cycles, the invoicing, and several other categories.

Using the accounting configuration options, you can do the following:

- [Change the business unit](#) (see page 139) (when applicable)
- [Set accounting configuration options](#) (see page 139)
- [Manage subscriptions](#) (see page 161)
- [Manage exchange rates](#) (see page 164)

Important! With one exception, CA Service Catalog sends emails in HTML format *only*. Therefore, to receive legible emails from CA Service Catalog, recipients must configure their email software, such as Microsoft Outlook, to accept emails in HTML format. Otherwise, emails from CA Service Catalog display indecipherable messages ("junk" characters) when opened. To help ensure that their end users can receive intelligible emails from CA Service Catalog, administrators *must* inform their end users of this requirement. If necessary, administrators must help them configure their email settings. The one exception to this HTML-only rule is *invoice history*. You can choose to view and email invoice history in HTML, CSV, or XML format. The HTML-only rule applies to all other invoice-related areas of CA Service Catalog, including invoice generation.

Change the Business Unit

By default, the settings that you view and update on accounting configuration pages apply to the business unit that you are logged in to. However, certain accounting configuration pages (for example, [Accounting configuration options](#) (see page 139) and [subscription management](#) (see page 161)) include the Change Business Unit button. If a page includes this button, you can optionally use this button to switch to a different business unit.

To change the business unit

1. Click the Change Business Unit button.

The Search Business Unit window appears.

2. Use the Expand and Collapse icons to navigate the business unit tree to locate the desired business unit. Alternatively, locate it by using the selection criteria and Search button.

Note: The results include *only* the business units permitted by your role.

3. Click the business unit name in the tree to select it.

The window closes and the configuration settings for that business unit appear.

You have changed the business unit.

Set Accounting Configuration Options

You can optionally customize several options for accounting configuration. These options cover invoicing and subscription details, to meet the requirements of your organization.

To set accounting configuration options

1. Log in as a user with the Service Delivery Administrator role.
2. Click Accounting, Configuration.

The Accounting Configuration page appears. On the left, in the Menu under the main menu, Options is selected. On the right, links appear for each category (subset) of the accounting configuration options.

3. Check the top (Welcome) line of the page for the name of the current business unit, and do one of the following:
 - To set the accounting configuration options for a different business unit, [change the business unit](#) (see page 139) before performing the next step.
 - To set the accounting configuration options for the current business unit, go directly to the next step.

4. Click the link for the category of options that you want to update, one of the following:

- [Accounting profile defaults](#) (see page 141)
- [Billing cycles](#) (see page 146)
- [General](#) (see page 146)
- [Invoice engine configuration](#) (see page 147)
- [Invoice methods](#) (see page 158)
- [Payment methods](#) (see page 159)
- [Subscription configuration](#) (see page 160)

The options appear for the category that you clicked.

5. View the options for the category, and click the Modify icon (by default, a pencil) for the option that you want to update.

The Edit Configuration dialog appears.

6. Update the setting as required and click Update Configuration to save your update.
7. Repeat the previous steps for each accounting configuration option that you want to update.

You have set the accounting configuration options. These settings apply to the children of the business unit that you updated, according to the [inheritance of configuration settings through the business unit hierarchy](#) (see page 118).

Accounting Profile Defaults

As part of [setting accounting configuration options](#) (see page 139), you specify the Accounting Profile Default settings. These settings indicate default values for newly created accounts for the current business unit. The following options require explanation:

Account Type

Specifies the type of account. This setting controls how outstanding balances are handled on invoices, as follows:

Open Item

Specifies that every invoice is unique. Once a charge appears on an invoice, it does not appear on any future invoices.

Balance Forward

Specifies that the remaining balance of a previous invoice is added to the next invoice.

Zero Balance

Specifies that the account is a zero balance account. A zero balance account can have charges appear on its invoice, but the total remaining balance is always zero. You cannot post payments to zero balance accounts.

This option is commonly used when an aggregating account holds the charges for one or more zero balance accounts.

Note: For details, see the *Administration Guide*.

Default: Open Item

Aggregate

Specifies the role of the account in charge aggregation for invoicing, as follows:

No

Specifies that the charges for the account appear *only* in the invoice of the account. The charges do *not* appear on an invoice for a related aggregating account.

Yes

Specifies that the charges for the account appear in the invoices for all of the following:

- The original account
- Each aggregating account in the same business unit or a parent business unit, up through the hierarchy of business units

Aggregating Account

Specifies that the invoice for the account shows charges for all accounts in the same business unit or child business units. These business units must have Aggregate set to Yes or Aggregating Account.

Note: To avoid double invoicing, do *not* specify more than one aggregating account in each business unit.

Default: No

Automatic Invoicing

Specifies whether to create an invoice for the account, as follows:

Yes

Specifies that the account has an invoice generated during a bill run.

No

Specifies that the account does not have an invoice generated during a bill run.

Default: Yes

Billing Cycle

Specifies the account invoicing cycle. Options are daily, weekly, and monthly.

Note: This field works with the Billing Cycle Interval, which is described later in this topic.

Default: Monthly

Period Start Date

Specifies how to set the start date for the invoice period for the account. Select from the following options:

Business Unit Opened Date

Sets the start date as the date the business unit of the account was created (the Opened Date).

Account Opened Date

Sets the start date as the date the account was opened (the Accounting Profile Opened Date).

Current Date

Sets the start date to be the date that the accounting profile (account) was created.

Current Date of Next Period

Sets the start date as the addition of both of the following:

- The date the accounting profile (account) was created
- The interval determined by the Billing Cycle and the Billing Cycle Interval

Day of Week

Sets the start date as the same day of the week on which the accounting profile (account) was created.

Day of Month

Sets the start date as the same day of the month on which the accounting profile (account) was created.

Day of Year

Sets the start date as the same day of the year on which the accounting profile (account) was created.

Day of Week Adjusted from Current Date

Sets the start date as the specified day of the next week after the accounting profile (account) was created.

Day of Month Adjusted from Current Date

Sets the start date as the specified day of the next month after the accounting profile (account) was created.

Day of Year Adjusted from Current Date

Sets the start date as the specified day of the next year after the accounting profile (account) was created.

Last Day of Current Month

Sets the start date as the last day of the month during which the accounting profile (account) was created.

First Day of Next Month

Sets the start date as the first day of the next month after the accounting profile (account) was created.

Specify Date

Sets the start date as the date that you specify manually.

Default: Account Opened Date

Billing Cycle Interval

Specifies the number of billing cycles between invoices.

For example, to bill the account quarterly, select a Billing Cycle of Monthly and a Billing Cycle Interval of 3. The Billing Cycle field is described earlier in this topic.

Default: 1

Default Days Due

Specifies the number of days after the invoice date to use as the payment due date.

Default: 10

Grace Days

Specifies the number of days permitted past the invoice date without a payment. If the invoice is not paid before the grace days expire, the account incurs additional fees and penalties.

Default: 10

Invoice Method

Specifies how to send invoices. Select one of the following options:

Email

Sends the invoice as an email attachment to the email address of the account.

The Catalog system does the following:

- Uses the format specified in Invoice Output Type setting
- Uses the delivery mechanism specified in the Invoice Generation Email Attachment Type setting
- Saves the attachment in the Invoice Email Location server folder

Fax

Saves the invoice using the format specified in Invoice Output Type setting in the Invoice Fax Location server folder.

Postal

Saves the invoice using the format specified in Invoice Output Type setting in the Invoice Postal Location server folder.

Printer

Saves the invoice using the format specified in Invoice Output Type setting in the Invoice Printer Location server folder.

Default: Email

Period End Date

Specifies how to set the end date for the invoice period for the account. Select one of the following options:

Compute from Start Date Using Billing Cycle

Specifies an end date based on the period start date, the billing cycle, and the billing cycle interval. Each of these settings is described earlier in this topic.

other options

Specifies an end date equivalent to the options for period start date. That setting is described earlier in this topic.

Note: The dates settings presume that each new day begins at a time of 00:00:00. Specify a Period End Date that includes the last full day of charges to include. For example, to bill for the entire month of July, make your period 7/1/yyyy - 8/1/yyyy to include the entire last day of the month.

Default: Compute from Start Date Using Billing Cycle

Status

Specifies the status of the account when it is created: Closed, Opened, or Suspended.

Invoicing occurs only when this setting is Opened.

Default: Opened

Status Reason

Specifies the reason for the value of the Status option. You enter this text manually.

Limit: 1024 characters

Default: New account waiting approval

Taxable

Specifies whether the account is taxable.

Specify Yes or No.

Default: No

Billing Cycles

As part of [setting accounting configuration options](#) (see page 139), you specify the settings for the billing cycles. You specify which billing cycle choices are available on the Accounting Profile of the account.

Daily

Specifies whether users can generate an invoice daily. If this option is set to Yes, Daily appears in the list of options for specifying the billing cycle. If it is set to No, Daily does not appear in the list.

Default: Yes

Monthly

Specifies whether users can generate an invoice monthly. If this option is set to Yes, Monthly appears in the list of options for specifying the billing cycle of the account. If it is set to No, Monthly does not appear in the list.

Default: Yes

Weekly

Specifies whether users can generate an invoice weekly. If this option is set to Yes, Weekly appears in the list of options for specifying the billing cycle of the account. If this option is set to No, Weekly does not appear in the list.

Default: Yes

General

As part of [setting accounting configuration options](#) (see page 139), you specify the General settings. These values apply to all accounts in the current business unit.

Default Post Payment Method

Specifies the default option for posting a payment: cash, check, or credit card.

Default: Check

Invoice Engine Configuration

As part of [setting accounting configuration options](#) (see page 139), you specify the Invoice Engine Configuration settings. These settings control the behavior of the invoice engine during bill runs. These values apply to transactions and invoices for all accounts in the current business unit. The following settings require explanation:

Invoice Style for Aggregation

Specifies how totals appear on invoices for aggregating accounts.

Select from the following options:

All Details

Displays all details appear.

Account Totals

Displays only the total of the aggregating account.

Drill Down Account Totals

Displays subtotals by account by service. Users can drill down to view details for each account.

Service by Account Totals

Displays subtotals by account by service, without drill-down functions.

Service Totals

Displays subtotals by service for all accounts.

Type by Account Totals

Displays subtotals by account by service option element type.

Type Totals

Displays subtotals by service option element type.

Default: All Details

Aggregate Advanced Charges

Specifies how advanced charges appear on an invoice. Advanced charges span multiple periods as defined by the period start and end dates in the Accounting Profile of the account.

Yes

Displays the total of the advanced charges on one line.

No

Displays the advanced charges individually on multiple lines.

For example, suppose the cycle for a subscription is monthly and the billing cycle for an account is yearly. In this case, a Yes setting summarizes the charges on one line. Conversely, a No setting displays 12 lines instead.

Default: Yes

Aggregate Current Charges

Specifies how to present current charges on an invoice. Current charges apply only to the current period as defined by the period start and end dates in the Accounting Profile.

Yes

Displays the total of the current charges on one line.

No

Displays the current charges individually on multiple lines.

This setting is similar to Aggregate Advanced Charges, but it applies to current charges instead.

Default: Yes

Allow No Activity Invoices

Specifies whether to generate invoices for accounts with no charges.

Yes

Generates invoices for *all* accounts, including accounts with no charges.

No

Generates invoices *only* for accounts with charges.

Default: No

Bill Run Capacity

Specifies the number of accounts to process for transaction and invoice generation until a commit is performed and all processing is persisted.

The larger the value, the more server memory is required and the faster the invoices are processed. The smaller the value, the less server memory is required, and the slower the invoices are processed.

Default: 100

Exclude Invoice Item

Specifies whether to include a chargeable item on an invoice if the quantity, unit cost, or both is 0.

Select from the following options:

Always Include

Invoices all items, regardless of the value for quantity and unit cost.

Where Quantity is 0

Exclude items when the quantity is 0.

Where Rate is 0

Exclude items when the unit cost is 0.

Where Quantity and Rate are 0

Excludes items when *both* the quantity and unit cost are 0.

Where Quantity or Rate is 00

Excludes items where *either* the quantity or unit cost is 0.

Default: Always Include

Uninvoiced Transactions

Specifies whether to include a transaction on an invoice. The decision is based on a comparison of the transaction date with the period start date and end date on the Accounting Profile of the account.

Select from the following options:

Include All Uninvoiced Transactions

Includes all transactions that have not yet been invoiced, regardless of transaction date.

Exclude Past Uninvoiced Transactions

Does not include transactions whose date is before the period start date, even if the transactions are not yet invoiced.

Exclude Future Uninvoiced Transactions

Does not include transactions whose date is after the period end date, even if the transactions are not yet invoiced.

Exclude Both Past and Future Uninvoiced Transactions

Does not include transactions whose date matches one of the following, even if the transactions are not yet invoiced:

- Before the period start date
- After the period end date

Both of these dates are outside the current period.

Default: Include All Uninvoiced Transactions

Invoice From Address

Specifies the address for the "From" field on the invoice.

Select from the following options: Service Provider Address and Business Unit Address.

Business Unit Address is available for a child business unit only.

Default: Service Provider Address

Invoice Generation Email Attachment Type

Specifies the delivery mechanism for the invoice when emails about invoices are sent.

Select from the following options:

Attachment

Includes the invoice as an attachment in the email. The format is specified in the Invoice Output Type setting.

Inline

Includes the invoice in HTML format in the text of the email.

Link

Includes a link to the invoice in the text of the email.

Default: Attachment

Invoice Generation Email Body Message

Specifies the body text for emails about invoices.

You can specify both literal text and dynamically substituted values.

The syntax for dynamically substituted values follows:

\$subject_name.variable_name\$

Specifies the name of the variable.

You can specify the following values:

- “statements” object:

statement_label - The label of the account plus an invoice statement ID, such as “acct1:10012”

period_from - The Accounting Profile Period Start Date of the account

period_to - The Accounting Profile Period End Date of the account

due_date - The due date of the invoice

- “billing_account” object:

account_label - The label of the account, such as “acct1”

Limit: 1024 characters

Default: Invoice Generated for \$statements.statement_label\$ for \$statements.period_from\$ - \$statements.period_to\$

Invoice Generation Email CC

Specifies the addresses of carbon copy (CC) recipients of emails about invoices.

You can specify multiple email addresses. Separate each email address with a semi-colon.

Limit: 1024 characters

Default: EMPTY

Invoice Generation Email From

Specifies the email address that sends emails about invoices.

Select from the following options:

User Defined

Specifies a custom email address that you enter manually. If you select this option but enter no email address, this setting changes to the literal value of EMPTY.

Service Provider Email

Specifies the email address of the service provider business unit.

System

Specifies that the Catalog system determines which one of the following email addresses to use: the Services Group or the super business unit.

Default: Service Provider Email

Invoice Generation Email Subject

Specifies the text for the subject line of emails about invoices.

You can specify both literal text and dynamically substituted values.

The syntax for dynamically substituted values is the same as the Invoice Generation Email Body Message setting. That setting is described earlier in this topic.

Limits: 1024 characters

Default: Invoice: \$statements.statement_label\$ processed for account: \$billing_account.account_label\$, Due date: \$statements.due_date\$

Invoice Generation Email To

Specifies the primary recipient of emails about invoices.

Select from the following options:

System

Uses the email address of the Send Invoice To field in the Accounting Profile of the account.

User Defined

Specifies a custom email address that you enter manually. If you select this option but enter no email address, this setting changes to the literal value of EMPTY.

You can specify multiple email addresses. Separate each email address with a semi-colon.

Default: System

Invoice History Email Attachment Type

Specifies the delivery mechanism for the invoice when you send emails from the Invoice History page.

Select from the following options:

Attachment

Includes the invoice as an attachment in the email. The format is specified in the Invoice Output Type setting.

Inline

Includes the invoice in HTML format in the text of the email.

Link

Includes a link to the invoice in the text of the email.

Default: Attachment

Invoice History Email Body Message

Specifies the body text for emails about invoices, when you send these emails from the Invoice History page.

You can specify both literal text and dynamically substituted values.

The syntax for dynamically substituted values follows:

\$object_name.variable_name\$

Specifies the name of the variable.

You can specify the same variables as for the Invoice Generation Email Subject setting.

In addition, you can specify the following variables:

- “invoice_history” object:
 - account_label - The label of the account

Limit: 1024 characters

Default: Invoices Generated During \$invoice_history.start_date\$ - \$invoice_history.end_date\$ total number of invoices:
\$invoice_history.num_invoices\$ number of phases processed = \$invoice_history.phases\$

Invoice History Email CC

Specifies the addresses of carbon copy (CC) recipients of emails from the Invoice History page.

You can specify multiple email addresses. Separate each email address with a semi-colon.

Limit: 1024 characters

Default: EMPTY

Invoice History Email From

Specifies the email address that sends emails about invoice history.

Select from the following options:

User Defined

Specifies a custom email address that you enter manually. If you select this option but enter no email address, this setting changes to the literal value of EMPTY.

Service Provider Email

Specifies the email address of the service provider business unit.

System

Specifies that the Catalog system determines which one of the following email addresses to use: the Services Group or the super business unit.

Default: System

Invoice History Email Subject

Specifies the text for the subject of emails from the Invoice History page.

You can specify both literal text and dynamically substituted values.

The syntax for dynamically substituted values follows:

\$object_name.variable_name\$

Specifies the name of the variable.

You can specify the same variables as for the Invoice Generation Email Subject setting.

In addition, you can specify the following variables:

- “invoice_history” object:
 - account_label - The label of the account

Limit: 1024 characters

Default: Invoices Generated During \$invoice_history.start_date\$ - \$invoice_history.end_date\$

Invoice History Email To

Specifies the primary recipient email addresses when emails are sent from the Invoice History page. You can specify multiple email addresses, separated by a semi-colon.

Limit: 1024 characters

Default: EMPTY

Invoice Email Location

Specifies a directory path on the local file system. This path stores invoices for the account when its Accounting Profile Invoice Method is set to Email.

Each invoice file name includes the account label and invoice statement ID.

For example, you could specify the following setting for a Windows environment:
%USM_HOME%\accounting\outbox\email.

Limit: 1024 characters

Default: EMPTY

Invoice Fax Location

Specifies a directory path on the local file system. This path stores invoices for the account when its Accounting Profile Invoice Method is set to Fax.

Limit: 1024 characters

Default: EMPTY

Invoice Postal Location

Specifies a directory path on the local file system. This path stores invoices for the account when its Accounting Profile Invoice Method is set to Postal.

Limit: 1024 characters

Default: EMPTY

Invoice Printer Location

Specifies a directory path on the local file system. This path stores invoices for the account when its Accounting Profile Invoice Method is set to Printer.

Limit: 1024 characters

Default: EMPTY

Invoice Output Type

Specifies the format to use when saving invoices as files.

Select from the following options:

- HTML
- CSV
- XML
- HTML and CSV
- HTML and XML

The file format you select is used for the previous two settings, Invoice Postal Location and Invoice Printer Location.

Default: HTML

Invoice Style

Specifies the style to use for viewing an invoice through the user interface.

Select from the following options:

- Style 1 - One option for invoice format.
- Style 2 - Another option for invoice format.

Default: Style 1

Invoice URL

Specifies an absolute URL path to the location that stores invoices for use by the Accounting, Invoices, Batch Printing menu option.

Limit: 1024 characters

Default: EMPTY

Output Invoices

Specifies whether to store the invoices for the account on the server file system, as follows:

With either setting, you can view invoices through the user interface.

Yes

Stores the invoices on the server file system. Depending on the Invoice Method setting, the invoices are stored in the locations indicated in the various "location" configuration settings.

No

Does not store invoices on the server file system.

Default: No

Payment Response

Specifies the text to print on an invoice when payment is posted.

Limit: 1024 characters

Default: Payment received - Thank you

Pro Rate Batch

Specifies whether to prorate invoice charges if the service start date does not align with the Accounting Profile period of the account, as follows:

No

Charges the invoice *only* after a full charge period has passed.

Yes

Prorates the charges.

For example, suppose that both of the following are true:

- This setting is Yes
- The charge and the Accounting Profile period of the account are both monthly

In this example, if you generate an invoice half way through the billing period, only half the charge appears on the invoice.

Default: Yes

Pro Rate Online

Specifies the same options as the previous setting (Pro Rate Batch), except that this setting applies to invoices that you view through the user interface.

Default: Yes

Use Time (requires restart)

Specifies whether to use the time portion of a transaction date and time stamp when determining the period for which to bill a transaction.

Default: Yes

Invoice Methods

As part of [setting accounting configuration options](#) (see page 139), you specify the Invoice Methods settings. These settings specify which methods of sending invoices are available on the Accounting Profile of the account.

Email

Specifies whether users can send invoices through email. If this option is set to Yes, Email appears in the list of options for specifying the delivery mechanism for invoices. If it is set to No, Email does not appear in the list.

Default: Yes

Fax

Specifies whether users can send invoices through fax. If this option is set to Yes, Fax appears in the list of options for specifying the delivery mechanism for invoices. If it is set to No, Fax does not appear in the list.

Default: Yes

Postal

Specifies whether users can send invoice through the postal service. If this option is set to Yes, Postal appears in the list of options for specifying the delivery mechanism for invoices. If it is set to No, Postal does not appear in the list.

Default: Yes

Printer

Specifies whether users can send an invoice by printing. If this option is set to Yes, Printer appears in the list of options for specifying the delivery mechanism for invoices. If it is set to No, Printer does not appear in the list.

Default: Yes

Payment Methods

As part of [setting accounting configuration options](#) (see page 139), you specify the Payment Methods settings. These settings specify which payment methods are available for applying a payment to an invoice.

Cash

Specifies whether Cash is a payment option for an invoice.

Default: Yes

Check

Specifies whether Check is a payment option for an invoice.

Default: Yes

Coupon

Specifies whether Coupon is a payment option for an invoice.

Default: No

Credit Card

Specifies whether Credit Card is a payment option for an invoice.

Default: Yes

Direct

Specifies whether Direct is a payment option for an invoice.

Default: No

Tip

Specifies whether Tip is a payment option for an invoice.

Default: No

Subscription Configuration

As part of [setting accounting configuration options](#) (see page 139), you specify the Subscription Configuration settings. These settings specify how the Catalog system handles subscriptions.

Default Subscribe State

Specifies the status to which the selected service options are set when an account is subscribed to a service, *one* of the following:

- Completed
- Pending

Default: Completed

Default Cancellation State

Specifies the status to which the selected service options are set when the subscription of an account to a service is cancelled.

Select from the following choices:

- Cancelled – Charges for the current billing period do not appear on the next invoice.
- Pending Cancellation – Charges for the current billing period appear on the next invoice, at which point the status is changed to Cancelled.

Default: Pending Cancellation

Default Subscription Page

Specifies the initial page displayed when the Subscriptions tab is selected.

Select from the following choices:

- Create New Subscriptions – Show catalog of services to which the account can subscribe.
- Existing Subscriptions – Show services to which the account is currently subscribed.

Default: Create New Subscriptions

Allow Instance Names

Specifies whether a name can be associated with a subscription instance.

If this option is set to Yes, when an account is subscribed to a service, you can optionally add some text to the subscription to name the instance.

If it is set to No, you cannot add text.

Default: No

Enable Subscription Notes

Specifies whether a note can be associated with a subscription instance.

If this option is set to Yes, when an account is subscribed to a service, you can optionally add notes to the subscription.

If it is set to No, you cannot add notes.

This setting is available for the service provider business unit only, and it applies to all business units.

Default: No

Manage Subscriptions

You can set subscription options that apply to services, service option groups, and service option elements. By default, these settings apply to all accounts. In addition, however, you can specify custom settings for one or more selected accounts.

To manage subscriptions

1. Click Accounting, Configuration.

The Accounting Configuration page appears. On the left, in the Menu under the main menu, Options is selected by default. On the right, links appear for each category (subset) of the accounting configuration options.

2. Review the top (Welcome) line of the page for the name of the current business unit, and do one of the following:
 - To manage subscription options for a different business unit, [change the business unit](#) (see page 139) before performing the next step
 - To manage subscription options for the current business unit, go directly to the next step
3. Click Subscription Management in the Menu on the left under the main menu.

The Subscription Decision Tree appears on the right, replacing the links for the accounting configuration categories.

4. Decide whether to update subscription options for all accounts in the business unit or only one more selected accounts. In either case, also decide whether to update subscription options for a specific service, service option group, or service option element.

To help you decide, review the following order of precedence:

- A setting for a service option element overrides the setting for the service option group to which it belongs.
- A setting for a service option group overrides the setting for the service to which it belongs.
- A setting for a specific account overrides the corresponding setting under “All Accounts.”

5. Do *one* of the following:

- Click All Accounts to apply your updates to every account in the business unit. The Services and Service Option Groups nodes appear, under all accounts.
- Click Apply to Individual Account to apply the updates to only one or more selected accounts in the business unit.

The Select Accounts dialog appears.

Select the account or accounts you want and click OK.

The Services and Service Option Groups nodes appear, under the selected accounts.

6. Click the Service or Services node (whichever you want to update), under either All Accounts or a selected account (whichever you specified in the previous step).
7. Drill down the Services and Service Option Group node to reach the [subscription management options](#) (see page 163) of interest. You can update the options for services, service option groups, and service option elements.

Note: You can optionally specify *no* value for Bill In Advance field or the Effective Dates And Bill Dates field when you create an account. In that case, the system applies default settings. Consequently, the account does *not* appear in the Subscription Decision tree. For information about creating accounts, see the *Administration Guide*.

8. Update these options as needed and save your changes.
9. Repeat the previous steps to update all the subscription management options you want. You can update subscriptions for all services, service option groups, and service option elements, or only the subscriptions for specific accounts.

You have managed subscriptions.

Note: These settings apply to any sub business units of the business unit that you are updating. If a business unit has sub business units, it has its own configuration settings.

Subscription Management Options

To [manage subscriptions](#) (see page 161), you specify the subscription management options, using the Subscription Decision Tree. You can specify separate settings that apply to all either *all* accounts in the business unit or to selected accounts *only*. In both cases, you use the tree to set the following options for individual services, service option groups, or service option elements:

Effective Dates and Bill Dates

Specifies when billing should begin after an account subscribes to a service option element. Select *one* of the following:

- Bill Date begins on the Effective Date – Begins billing the account on the date the subscription is made.
- Specify a Bill Date separate from the Effective Date – Begins billing the account on a specific date, regardless of the subscription date.
- Specify a Bill Date relative to the Effective Date – Begins billing the account based on the *complex* option you specify, relative to the subscription date. An example is “the first day of the month of the subscription.”
- Specify a Bill Date offset from the Effective Date – Begins billing the account based on the “before and after” option you specify, relative to the subscription date. An example is “two months after the subscription date.”

Bill in Advance

Specifies whether a subscribing account is charged in advance of a service being rendered. Select *one* of the following:

- Do not bill in advance – Bills the account when the service is rendered.
- Specify how far in advance the charge should be billed – Bills the account the specified number of periods in advance.

Note: The billing period is the billing period of the service option element being subscribed to, not the account's billing cycle.

For example, suppose a service option element specifies a Unit Cost of \$10 with a Billing Cycle of Periodic, a Periodic Type of Monthly, and a Periodic Type Interval of 1. If this setting is 3, then a subscribing account is billed \$30 on the first invoice and each interval invoice, rather than \$10 per month.

Exchange Rates

CA Service Accounting supplies the Accounting, Configuration, Exchange Rates table. By default, this table displays exchange rates for the current time period. You can also view any previously defined exchange rates for earlier or future periods.

Using this table, you [manage exchange rates](#) (see page 164) for the currencies used in your implementation, relative to the US dollar. The Catalog system uses these exchange rates to produce invoices for each account in the currency of the business unit to which the account belongs.

All exchange rates are relative to the US dollar. When you convert from one currency type to another, the system first converts the catalog amount to US dollars. Next, the system converts the amount to the currency type of the account.

During installation, the exchange rates for all currency types are set to 1.0. This setting means that the exchange rate for each currency type relative to the US dollar is 1.0.

Updates to exchange rates apply to the *entire* system. You *cannot* specify different exchange rates for different business units.

Manage Exchange Rates

You can update [exchange rates](#) (see page 164) in CA Service Accounting as the official exchange rates change for the countries and currencies with which you do business. Updates to exchange rates apply to the *entire* system. You *cannot* specify different exchange rates for different business units.

To manage exchange rates

1. Click Accounting, Configuration.

The Accounting Configuration page appears. On the left, in the Menu under the main menu, Options is selected by default. On the right, links appear for each category (subset) of the accounting configuration options.

2. Click Exchange Rates in the Menu on the left under the main menu.

The Exchange Rates table for the current date range appears on the right, replacing the links for the accounting configuration categories. The table lists the currency name, symbol, date, exchange rate, and so forth. By default, The table for the current time period (the previous month) appears.

3. View the exchange rates for the currency defined in your system.
4. Complete the following actions if applicable. If an action does not apply, skip it.
 - [Display exchange rates for a date range](#) (see page 165)
 - [Edit exchange rates for the current time period](#) (see page 166)
 - [Delete an exchange rate for a date range](#) (see page 167)
 - [Delete a currency name from the exchange rate table](#) (see page 168)
 - [Add a new exchange rate for a date range](#) (see page 169)

You have managed exchange rates.

Display Exchange Rates for a Date Range

You can view exchange rates for past time periods. Doing so can help you review invoices for previous billing periods.

To view the exchange rates for a specific date range

1. Complete the initial steps of [managing exchange rates](#) (see page 164), until you display the Exchange Rates table.

The Exchange rate table appears.

2. Click the Select Date button on that table.
3. Enter the date range for the exchange rates that you want to view, and click OK.

The exchange rates for that period appear.

You have viewed the exchange rates.

Edit Exchange Rates for the Current Time Period

You can optionally modify the exchange rates for any or all currency types relative to the US dollar, for the current time period. You can do so, for example, to provide a regularly scheduled update or to correct a mistake in the initial setup.

To edit exchange rates for the current time period

1. Complete the initial steps of [managing exchange rates](#) (see page 164), until you display the Exchange Rates table.

The Exchange rate table appears.

2. Select the currency types whose exchange rate you want to update, and click Edit.

The Exchange Rate field opens for editing for all currency types.

3. Enter the new exchange rate for each currency type that you want to update, relative to the US dollar, in the Exchange Rate field.

4. Click Save.

The Catalog system saves your changes.

You have edited the exchange rates, and the values that you updated appear on the page.

Delete an Exchange Rate for a Date Range

You can delete an exchange rate for a date range from the Exchange Rates table. You can do so, for example, to correct an initial error or if you are certain that your implementation does not need the exchange rate.

Important! Deleting *all* exchange rate entries for a currency name deletes that currency name from the Exchange Rates table completely! You *cannot* use the GUI to restore a deleted currency name. Therefore, use caution when deleting exchange rates from the table.

You can, however, intentionally [delete a currency name from the exchange rate table](#) (see page 168) if you are certain that you want to do so.

To delete an exchange rate for a date range

1. Complete the initial steps of [managing exchange rates](#) (see page 164), until you display the Exchange Rates table.

The Exchange rate table appears.

2. Select each exchange rate that you want to delete. Verify that you do *not* unintentionally delete *all* exchange rates in the table for any currency name, as noted in the introduction to this topic.

3. Click the Delete link.

You are prompted to confirm the deletion.

4. Click OK.

The Catalog system saves your changes.

You have deleted the selected exchange rates.

Delete a Currency Name

You can delete currency names from the Exchange Rates table. You can do so, for example, to correct an initial error or if you are certain that your implementation does not need the currency.

Note: Delete currency names with caution, because you *cannot* use the GUI to add a missing or deleted currency name.

To delete a currency name from the exchange rate table

1. Complete the initial steps of [managing exchange rates](#) (see page 164), until you display the Exchange Rates table.

The Exchange rate table appears.

2. Select each currency name that you want to delete. If a currency name has multiple options, select all of them.

3. Click the Delete link.

You are prompted to confirm the deletion.

4. Click OK.

The Catalog system saves your changes.

You have deleted the selected currency names.

Add a New Exchange Rate for a Date Range

You can add a new exchange rate for a new date range. You can do so, for example, to provide a periodic update or to prepare for the start of the next billing period.

Note: You *cannot* add a new exchange rate that overlaps the same date range as any existing exchange rate.

To add a new exchange rate for a date range

1. Complete the initial steps of [managing exchange rates](#) (see page 164), until you display the Exchange Rates table.
The Exchange rate table appears.
2. Select each currency name for which you want to add an additional exchange rate.
The Catalog system adds new exchange rate rows for each selected currency name.
3. For each new exchange rate row, complete the following fields:
 - Currency Name
 - Currency Symbol
 - Date
 - Exchange Rate
4. Click Save.
The Catalog system saves your changes.

You have added a new exchange rate for a date range.

Set Service Builder Configuration Options

You configure Service Builder to customize settings for request management, access control, request emails, and so forth. These settings specify how the Catalog system processes requests in your organization.

To set Service Builder configuration options

1. Click Service Builder, Configuration.
The Service Builder Configuration page appears. On the left, in the Menu under the main menu, the Options column lists the links for each category (subset) of options.
2. Do one of the following:
 - To manage configuration options for a different business unit, [change the business unit](#) (see page 171) before performing the next step
 - To manage configuration options for the current business unit, go directly to the next step

3. Click the link for the category of options that you want to update, one of the following:

- [Catalog configuration](#) (see page 172)
- [Request management configuration](#) (see page 173)
- [System configuration](#) (see page 185)

The options appear for the category that you clicked.

4. View the options for the category, and click the Modify icon (by default, a pencil) for the option that you want to update.

The Edit Configuration dialog appears.

5. Update the setting as required and click Update Configuration to save your update.
6. Repeat the previous steps for each Service Builder configuration option that you want to update.

You have set the Service Builder configuration options. These settings apply to the children of the business unit that you updated, according to the [inheritance of configuration settings through the business unit hierarchy](#) (see page 118).

Important! With one exception, CA Service Catalog sends emails in HTML format *only*. Therefore, to receive legible emails from CA Service Catalog, recipients must configure their email software, such as Microsoft Outlook, to accept emails in HTML format. Otherwise, emails from CA Service Catalog display indecipherable messages ("junk" characters) when opened. To help ensure that their end users can receive intelligible emails from CA Service Catalog, administrators *must* inform their end users of this requirement. If necessary, administrators must help them configure their email settings. The one exception to this HTML-only rule is *invoice history*. You can choose to view and email invoice history in HTML, CSV, or XML format. The HTML-only rule applies to all other invoice-related areas of CA Service Catalog, including invoice generation.

Change the Business Unit

By default, the Catalog system displays settings for the business unit that you logged in to. You can optionally change to a different business unit, if your role permits you to do so.

Note: When common multi-tenant administration is enabled, you can add or delete tenants, or edit their common attributes *only* through CA Service Desk Manager *not* CA Service Catalog. When common multi-tenant administration is enabled, you can *view* tenants and all their attributes in CA Service Catalog, but you can edit only the CA Service Catalog-specific attributes. For details about common multi-tenant administration, and about roles, see the *Administration Guide*.

To manage the configuration settings for a different business unit

1. Click Service Builder, Configuration.
The Service Builder Configuration page appears. On the left, in the Menu under the main menu, the Options column lists the links for each category (subset) of options.
2. Click the Change Business Unit button.
The Search Business Unit dialog appears.
3. Use the Expand and Collapse icons to navigate the business unit tree. Alternatively, use the selection criteria and Search button to locate the desired business unit.
Note: The list includes only the business units that your role permits you to access.
4. To select a business unit, click its name in the tree.
The window closes, and the configuration settings for that business unit appear.

Catalog Configuration Options

As part of [setting the Service Builder configuration options](#) (see page 169), you specify the following Catalog Configuration options. These settings control the behavior of the catalog.

Pass Through Catalog

Specifies whether to include the catalog of the parent business unit.

If you select this option, the parent catalog is passed down to the child business unit. This setting is useful in a multiple-level business unit organization and applies only to the settings for a child business unit.

Default: No

Default Effect of Service Option Element Changes

Specifies when to reflect changes to service option elements for accounts that have subscribed to or requested services that include them.

Select one of the following options to use when the service option element changes:

Specify when the Service Option Element Changes - Allow User to Choose

Enables the administrator to specify the effect of the change on existing subscribers or requestors.

Beginning of Accounts' Current Billing Period - No Audit Trail

Implements the change retroactively to the beginning of the current billing period for existing subscribers or requestors. No audit trail applies.

Beginning of Accounts' Current Billing Period

Implements the change retroactively to the beginning of the current billing period for existing subscribers or requestors.

Beginning of Accounts' Next Billing Period

Implements the change at the beginning of the next billing period for existing subscribers or requestors.

Immediately during Accounts' Billing Period

Implements the change immediately for existing subscribers or requestors.

Specify a Future Effective Date

Enables the Administrator to specify a date on which the change takes effect for existing subscribers or requestors.

Default: Specify when the Service Option Element Changes - Allow User to Choose.

Request Management Configuration Options

As part of [setting the Service Builder configuration options](#) (see page 169), you specify the Request Management Configuration options. These settings that control the behavior of requests for the following groups of parameters:

- [Access Control parameters](#) (see page 173)
- [Other parameters](#) (see page 176)
- [Request Email parameters](#) (see page 182)

Access Control Parameters

As part of [setting the Service Builder configuration options](#) (see page 169), you specify the following Access Control parameters:

Access Control: Add Request

Specifies which user roles can add a request.

Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, End User, Catalog User, Request Manager, Catalog Administrator

Access Control: Edit Request

Specifies which user roles can edit a request. All users can edit their own requests, as long as the status of the request is in the not submitted range.

Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, End User, Catalog User, Request Manager, Catalog Administrator

Access Control: Delete Request

Specifies which user roles can delete a request or a requested service. All users can delete their own requests, as long as the status of the request is in the not submitted range. Once a requested service is in a canceled state, only users with Delete Request permission can delete a canceled service.

Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator

Access Control: Cancel Request

Specifies which user roles can cancel a request.

This parameter works together with the Allow Cancellation Through parameter, which is described later in this list.

Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator

Access Control: Show Amount Column

Specifies which user roles can view the Amount Column when viewing a request.

Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator

Access Control: Show Period Column

Specifies which user roles can view the Period Column when viewing a request or shopping cart.

Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator

Access Control: Show Related Ticket Column

Specifies which user roles can view the Related Ticket Column when viewing a request or shopping cart.

Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator

Access Control: Show General Information

Specifies which user roles can control whether the general information form is visible when you create a request.

Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator, Service Manager, End User, Catalog User

Access Control: Show Request Information

Specifies which user roles can control whether the request information form is visible when you create a request.

Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator, Service Manager, End User, Catalog User

Access Control: Save Cart As Request

Specifies which user roles can view the button allowing the user to save the shopping cart as a request, clearing the cart for reuse.

Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator

Access Control: Proxy Request

Specifies which user roles can view the link to change the Requested For field from your own user ID or account to another user ID or account.

Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator

Access Control: Proxy Action

Specifies which user roles can see the link to approve, reject, fulfill, or transfer requests pending action assigned to other users.

Access Control: Show Fulfillment Details

Specifies which user roles can view statistical information regarding the time required to fulfill a service option in the past.

Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator

Access Control: Take/Return Request Pending Action

Specifies which user roles can take or return ownership of requests pending action. They can take ownership of requests pending action from both of the following:

- A group queue
- The queue of another user in the same business unit or child business unit

Similarly, they can return ownership of requests pending action from their own queue to their group queue.

Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator

Access Control: Transfer Request Pending Action

Specifies which user roles can transfer ownership of requests pending action from the assigned user to either of the following:

- Another user in the same group
- Another user in the same business unit or child business unit

Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator

Access Control: Delegate Request Pending Action

Specifies which user roles can delegate ownership of requests pending action from a group queue to either of the following:

- A specific user in that group
- Another user in the same business unit or child business unit

Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator

Access Control: Push Through Requests

Specifies which user roles can push through ("force") a stuck request to the next level of approval or fulfillment.

Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator

Access Control: Display Request Warning

Specifies which user roles can view the warning icon indicating that a request is stuck. Conversely, if a catalog user cannot access to this option, then that user does not see the warning icon, even if the request is stuck.

Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator, End User, Catalog User

Access Control: Hold/Resume Request

Specifies which user roles can hold a request that is in progress and can resume a request that is in Hold status.

Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, Request Manager, Catalog Administrator, End User, Catalog User

Other Parameters

As part of [setting the Service Builder configuration options](#) (see page 169), you specify the following miscellaneous parameters:

Allow Cancellation Through

Defines the status through which users can cancel requests. After the request moves to the next status, it cannot be canceled.

This parameter works together with the Access Control: Cancel Request parameter described earlier in this list.

Default: Fulfilled

You can [customize the list of request statuses](#) (see page 280).

Allow Discrete Handling for Reject

Specifies the effect of the rejection of a single service or service option upon other services and service options in the same request, as follows:

Yes

Specifies that when you reject a service or service option, the remaining services or service options can advance if they are approved. That is, if the following are approved, they can advance in the request lifecycle:

- Other services in the same request
- Other service options in the same service

No

Specifies that when you reject a service or service option, the entire request is rejected. That is, all services in the same request are rejected and can no longer advance in the request lifecycle, even if they were previously approved. Similarly, all service options in the same service are rejected and can no longer advance in the request lifecycle, even if they were previously approved.

The default is No, for backward compatibility. With this setting, the request lifecycle functions the same as it did in past releases of the product before this parameter was implemented.

Note: For more information about using a discrete request lifecycle, including sample settings and their meanings, see the *Administration Guide*.

Allow Discrete Handling of Service Options After

Specifies the status at which request managers (approvers and fulfillers) can handle requests pending action (approval, rejection, or fulfillment) *discretely*. When the request reaches the status you specify, request managers can discretely (individually) approve, reject, or fulfill each service option in every service in the request.

In other words, you can use this parameter to specify that pending actions are assigned at the service option level, rather than the service level.

The setting you specify applies to the request *from* the starting status that you specify *through* the remainder of the request lifecycle.

Valid values are Submitted, Pending Fulfillment, or Completed.

The default is Pending Fulfillment, for backward compatibility. With this setting, the request lifecycle functions the same as it did in past releases before this parameter was implemented.

Note: For more information about using a discrete request lifecycle, including sample settings and their meanings, see the *Administration Guide*.

Allow Discrete Request Life Cycle After

Specifies the status at which individual service options in a service and individual services in a request advance to further statuses in the request lifecycle independently. Here, *independently* means *without* requiring or waiting for any other service option in the same service or any other service in the same request to advance its status.

As soon as the request reaches the status that you specify, the service options that you approve or fulfill can complete the remainder of the request lifecycle. This condition exists even if other service options in the same service do not advance in status.

Similarly, as soon as the request reaches the status that you specify, the services that you approve or fulfill can complete the remainder of the request lifecycle. This condition exists even if other services in the same request are rejected or are not updated.

Valid values are Submitted, Pending Fulfillment, or Completed.

The default is Completed, for backward compatibility. With this setting, the request lifecycle functions the same as it did in past releases of the product before this parameter was implemented.

The setting you specify applies to the request *from* the starting status that you specify *through* the remainder of the request lifecycle.

Note: For more information about using a discrete request lifecycle, including sample settings and their meanings, see the *Administration Guide*.

Allow Notes at Service Option Level

Controls whether a user can add notes at the service and service option levels.

If this option is set to Yes, then the Add Note icon appears in the Action column for requests. Therefore, the user can add a note for a specific service or service option. If this option is set to No, then the user can add notes for the entire request but not for a specific service or service option.

Default: No

Allow Only One Service Per Request

Specifies whether a user can include more than one service in a request or cart.

If this option is set to Yes, then a user can have only one service in a cart or request. Also, the user must submit the cart or request before creating a new one.

If this option is set to No, then a user can select multiple services from the catalog. The user can add them to the cart or request before submitting the request.

Default: No

Browse Catalog Layout

Specifies whether to use the standard look-and-feel or a grid-view look-and-feel for the page on which users create, customize, and submit requests. Specify *one* of the following:

Default

Specifies the standard look-and-feel.

Grid View

Specifies the grid-view look-and-feel.

Browse Catalog: Show Folder Icons

Specifies whether images associated with catalog folders appear in the Browse section of the Requests page.

If this option is set to Yes, folder images appear in the Browse section. If this option is set to No, they do not appear.

Default: No

Browse Catalog: Show Subfolders

Specifies whether the top level subfolders under each catalog folder appear in the Browse section of the Requests page.

If this option is set to Yes, the first-level of subfolders appear under each catalog folder in the Browse section. If this option is set to No, only the catalog folders appear.

Default: Yes

Note: For any individual catalog folder, you can override this default by changing its folder details on the Service Builder, Services page. For details, see the *Administration Guide*.

Default User for Request Actions

Specifies the user who to be assigned a pending action when no other user is available. This setting is typically used for request approvals when the user needs manager approval and no manager exists in the system for the user.

Note: When this setting is used with the system approval process, verify that this user has the highest authorization level. For details, see the *Administration Guide*.

Default: spadmin

Display Service Health

This parameter applies *only* if you are integrating CA Service Catalog with CA Business Service Insight!

Specifies whether to enable catalog users requesting a service to view actual, current data regarding the quality or "health" of a service. The health is based on the level of compliance of the service to its associated metrics. This data includes the contractual metrics, incentive metrics, and the SLA health period. This information is specified in the contract-specific details for the service option elements in the service being requested.

The metric data includes both the performance criteria and the actual number of violations, including the time increments measured.

If you enable this option, catalog users can view this actual, current metric data for the service they are requesting. Conversely, if you do not enable this option, catalog users requesting a service cannot view this information for the service they are requesting.

Note: For details about integrating CA Service Catalog with CA Business Service Insight, see the *Integration Guide*.

Enable Delegation of Catalog

Specifies whether to enable the delegation of catalogs: Yes or No.

When this option is enabled, no users are *required* to delegate use of their catalogs, but they can *optionally* do so.

Note: The delegation of a catalog does *not* affect the Catalog configuration of the Service Builder, such as the Use Service Provider Catalog Only and Pass Through Catalog configuration parameters. Similarly, the delegation of a catalog is *not* directly related to the configuration options (such as Access Control: Add Request) in this Request Management Configuration section. For details about delegation of catalogs, see the *Administration Guide*.

Notify users when they complete their own pending actions

Specifies whether request managers receive a notification email every time they address a pending action by approving, rejecting, or fulfilling a service option, service, or request.

If you specify Yes, request managers receive such emails confirming their own actions.

If you specify No, request managers receive no such emails.

This setting is especially relevant if you are using discrete approval and the Allow Request Life Cycle to Continue After parameter is set to Submitted. In that case, if the Notify users when they complete their own pending actions parameter is set to Yes, request managers are likely to receive several notification emails.

For example, if a service has five service options and the request manager approves each option, the request manager receives five confirmation emails. To prevent request managers from receiving such emails, set Notify users when they complete their own pending actions to No.

The Requested For users and Requested By users always receive these notification emails, regardless of the setting of these parameters.

Note: For details about using a discrete request lifecycle, see the *Administration Guide*.

Number of Requests per Page

For individual users (not administrators), specifies the maximum number of requests that appear on Request List pages. When a user moves to a new Request List page, the default setting replaces their custom settings. Users can optionally customize the display for each new Request List page they view.

Request List pages appear when you click Home, Requests and click any of the following options:

- Open Requests
- My Recent Requests
- Completed Requests
- Pending My Action

Advanced Search—after you search for requests and view the results

Note: Administrators can set the following options for all users: The individual columns that appear on Request List pages and the default maximum number of requests per page. For details, see the *Administration Guide*.

PDA Support: Enable

Specifies whether to enable PDA support: Yes or No.

When you specify Yes, PDA users can click the links provided in PDA-compliant request approval emails to access the requests and approve or reject them. Support for forms limited when you enable PDA Approval.

When you specify No, the links for accessing the requests and approving or rejecting them do *not* appear in the request approval emails that PDA users receive. The absence of such links implicitly guides PDA users to use an office computer to view, approve, and reject requests as needed.

Note: For details about using PDA support, including the limitations, see the *Administration Guide*.

Request Home Page: Include Request Information

Specifies which roles can view the Request Lookup and My Recent Requests sections on the Home or Requests menu option page.

Default: Service Delivery Administrator, Super Business Unit Administrator, Administrator, End User, Catalog User, Request Manager, Catalog Administrator

Request Email Parameters

As part of [setting the Service Builder configuration options](#) (see page 169), you specify the following Request Email parameters:

Request Email: From Address

Specifies the email address from which the Catalog system sends emails about requests, one of the following:

User Defined

Uses the email address specified by the user. Selecting this option with no email address specified sets this setting to EMPTY.

Service Provider Email

Uses the email address for the service provider business unit.

Default: CatalogSystem@serviceprovider.com, where “*serviceprovider*” is the root business unit specified during installation.

Request Email: From Name

Specifies the email address *name* from which emails about requests are sent.

Default: CatalogSystem

Request Email: To

Specifies the primary recipient email address to which emails about requests are sent, one of the following:

User Defined

Uses the email address specified by the user. Multiple email addresses can be specified, separated by a semi-colon. Selecting this option with no email address specified sets this setting to EMPTY.

Requested For User/Account Email

Uses the email address of the user or account to which this request applies.

Requested By User/Account Email

Uses the email address of the user or account that created this request.

Default: EMPTY, meaning this value is set when email options are used.

Request Email: CC

Specifies the “CC” recipient email address to which emails about requests are sent, one of the following:

User Defined

Uses the email address specified by the user. Multiple email addresses can be specified, separated by a semi-colon. Selecting this option with no email address specified sets this setting to EMPTY.

Requested For User/Account Email

Uses the email address of the user or account to which this request applies.

Requested By User/Account Email

Uses the email address of the user or account that created this request.

Default: EMPTY, meaning this value is set when email options are used.

Request Email: BCC

Specifies the “BCC” recipient email address to which emails about requests are sent, one of the following:

User Defined

Uses the email address specified by the user. Multiple email addresses can be specified, separated by a semi-colon. Selecting this option with no email address specified sets this setting to EMPTY.

Requested For User/Account Email

Uses the email address of the user or account to which this request applies.

Requested By User/Account Email

Uses the email address of the user or account that created this request.

Default: EMPTY, meaning this value is set when email options are used.

Request Email: Subject

Specifies the email subject used when emails about requests are sent.

In addition to specific text, you can include dynamically substituted values in the subject text. The syntax for including dynamically substituted values is `$Request.variable_name$`.

variable_name

Specifies the name of the variable value to use.

You can specify the following variables in the subject text:

request_id

Specifies the internal Request ID, such as "10001".

name

Specifies the request name entered by the user.

status

Specifies the status of the request, such as "Pending Approval."

created_date

Specifies the date and time the request was created.

modified_date

Specifies the date and time the request was last modified.

completion_date

Specifies the date and time the request was completed.

desired_date

Specifies the date and time in the Date Required field of the request.

comments

Specifies the request Description specified by the user.

priority

Specifies the priority of the request.

req_for_account_id

Specifies the internal account ID for the Requested For user or account.

req_by_account_id

Specifies the internal account ID for the Requested By user or account.

req_for_user_id

Specifies the user ID of the Requested For user, if the request is for a user not an account.

req_by_user_id

Specifies the user ID of the Requested By user.

Default: Email of Request (\$Request.request_id\$) - \$Request.name\$

Request Email: Message

Specifies the email message used when emails about requests are sent. You can override this text.

In addition to specific text, you can include dynamically substituted values in the subject text. The syntax for including dynamically substituted values is \$Request.variable_name\$.

variable_name

Specifies the name of the variable value to use.

The variables available for use are the same as in the Request Email: Subject setting.

Default: Request (\$Request.request_id\$) created on \$Request.created_date\$

System Configuration

As part of [setting the Service Builder configuration options](#) (see page 169), you specify the following System Configuration parameters. These settings control the behavior of the system, regardless of business unit. This category is displayed *only* when you are logged in to the service provider (root) business unit.

Use Service Provider Configuration Only

Specifies whether a child business unit can have its own Service Builder configuration settings.

If this setting is Yes, the Catalog system ignores all Service Builder configuration settings for a business unit. Consequently, each business unit uses the configuration settings for the service provider.

If this setting is No, then each business unit can have its own Service Builder configuration settings.

Default: No

Use Service Provider Catalog Only

Specifies whether the service provider business unit catalog is available to all business units in the hierarchy.

If this setting is Yes, the subscribing or requesting user of a child business unit sees only the catalog of the service provider (root) business unit. That is, the child business unit cannot have its own catalog.

If this setting is No, the child business unit can have its own catalog.

Default: No

Configuration of Web Services

CA Service Catalog provides a comprehensive web service API. Each web service provides a set of operations or methods related to a particular object type. By default, all methods for all web services are deployed. However, you can optionally undeploy selected web services. You can also redeploy methods that you previously undeployed.

Note: For instructions to use and configure the web services, see the *Administration Guide*.

Single Location for Shared Files

If you have installed Service View on multiple computers (either clustered or nonclustered), we recommend that you [set up](#) (see page 187) a single location for shared files. Shared files can include documents, reports, images of services, data mediation files, customizations, and forms.

By default, the location for shared files is the %USM_HOME%\filestore folder on *every* Service View computer; this folder contains several subfolders. However, for optimal efficiency, you can specify *one* location on a single computer that all Service View computers share. This single location is named the *central filestore* or *filestore*. The computer on which the filestore resides can have Service View installed. However, Service View is not required on that computer.

If you have installed Service View on multiple computers and you do not set up a filestore, then verify that the individual filestores on all Service View computers are synchronized.

If you have installed Service View on a single computer, this entire process does not apply, so you can skip it.

Set Up a Single Location for Shared Files

If you have installed Service View on multiple computers (either clustered or nonclustered), we recommend that you set up a [single location for shared files](#) (see page 186). Doing so helps improve the accuracy and efficiency of sharing files between computers.

To set up a single location for shared files

1. Meet the following prerequisites:
 - Verify that all computers on which Service View is installed have a trusted domain relationship. This trusted relationship enables user accounts and global groups to be used in a domain other than the domain where the accounts are defined.
 - Start the CA Service View service with the login credentials (user name and password) of the Windows user that has read/write access to the shared location. If necessary, change the login credentials for the CA Service View service to meet these requirements, as follows:
 - a. In the Windows Control Panel, right-click the service, click Properties, click the Log On tab, and enter the login credentials.
 - b. Save the changes and restart the service.

Note: For details about updating Windows services, see your Windows documentation.

2. Decide whether to keep the default location, the %USM_HOME%\filestore folder on the first Service View computer, as the filestore for all Service View computers. Proceed as follows:
 - To keep the *default* filestore, share the %USM_HOME%\filestore folder on the first Service View computer. Verify that the Windows operating system users who are updating the filestore have read/write access to this folder. For details about creating Windows shares, see your Windows documentation.

You are now finished setting up the filestore, and the remaining steps in this topic do not apply.
 - To set up a *new* location for the filestore, perform all the remaining steps in this topic.
3. [Perform the prerequisite tasks for setting up a custom location for the filestore](#) (see page 188).
4. Select Administration, Configuration, Filestore Information.

The Administration Configuration page appears, with the Filestore Information settings in view.

5. Do the following:
 - a. Click the Edit (pencil) icon for the Filestore Location variable.
The Edit Configuration dialog appears.
 - b. In the Filestore Location field, specify the UNC path name of the shared drive you defined in a previous step, for example:
`\\big-computer\Shared_USM\filestore` or `\\big-computer\filestore`.
 - c. Click Update Configuration.
 - d. Click Test to verify the validity of the share.
This test returns a successful connection test message if the filestore can be used to store files uploaded by users.
Important! Testing the filestore is required!
6. Perform the action that applies:
 - If the test succeeds, copy the entire contents of the `%USM_HOME%\filestore` folder to the new location.
 - If the test fails, reconfigure the share. Also, verify that all the Service View services that are accessing the share have the same, valid credentials.
7. Recycle all Service View services on all computers.
8. If you are using vertical clustering, recycle each Service View service on each individual vertical cluster node separately.

Note: If you later move the shared folder to another new location, repeat these steps to set up the new location.

Perform the Prerequisite Tasks

If you do not use the default location for the [filestore](#) (see page 187), perform the prerequisite tasks to set up a custom location, as explained in this topic. Otherwise, skip this topic.

To perform the prerequisite tasks to set up a custom location for the filestore

1. Decide the computer and the folder on it to use as the filestore.
2. Share this folder.
3. Verify that the Windows operating system users who are updating the filestore have read/write access to this folder.
4. Use the UNC path in the format `\\computer-name\folder-name` to specify the location of the filestore.
5. Start the Service View service with the logon credentials of the Windows user who requires access to the folder.

6. Verify that these users can log in to all Service View computers and have read/write access to the filestore.

You have performed the prerequisite tasks to set up a custom location for the filestore.

Advantages of 64-Bit Mode

64-bit systems are more powerful than 32-bit systems, mainly because of the large amount of RAM they support (more than 4 GB) and their efficient memory management. To exploit *all* of the available RAM on a 64-bit operating system, run a 64-bit JRE. A 32-bit JRE can use *only* 2 GB or less of the available RAM, even on a 64-bit operating system. For these reasons, running software on 64-bit systems rather than 32-bit systems can increase the performance of your applications.

CA Service Catalog products and components are installed as 32-bit applications and run in that mode by default. To exploit the power of 64-bit mode completely, install these components on a 64-bit operating system and [configure them to run in 64-bit mode](#) (see page 189). Afterwards, you can optionally reconfigure them to run in 32-bit mode again, if required.

Note: 64-bit mode is supported *only* when CA Service Catalog is installed on the Apache Jakarta Tomcat web server. You can optionally install CA Service Catalog on 64-bit operating systems. For details about supported 64-bit operating systems and database software, see the *Release Notes*.

Configure Components to Run in 64-Bit or 32-Bit Mode

You can optionally configure CA Service Catalog components to run in 64-bit mode, because of the [advantages](#) (see page 189) of doing so, especially improved performance. You can also reconfigure them to run in 32-bit mode, if necessary.

Follow these steps:

1. Verify that CA Service Catalog is installed on a 64-bit operating system, on the Apache Jakarta Tomcat web server.

Note: Perform the remaining steps on every computer that has a CA Service Catalog product or component installed, one computer at a time.

2. Verify that a 64-bit Java Runtime Environment (JRE) is installed locally.

If you have not already installed a 64-bit JRE from the CA Service Catalog installation media, do so now. This JRE is located under the Utilities\Java\amd64 folder.

3. Record the path name of this 64-bit JRE for later use.
4. Use the Windows Control Panel, stop these services: CA Service View, CA Service Accounting, CA Service Fulfillment, and Message Queue 4.1 Broker.
5. Click Start, Programs, CA, Service Catalog, Service Catalog Command Prompt.

The CA Service Catalog command prompt opens.

- a. Enter one of the following ant commands at the CA Service Catalog command prompt:

- Enter this command to change to 64-bit mode:

```
ant switch-to-64-bit
```

- Enter this command to change to 32-bit mode (the default mode):

```
ant switch-to-32-bit
```

- b. Enter the path name of the 64-bit or 32-bit JRE when prompted.
- c. Wait for the ant command to complete successfully.

The ant command [makes several updates](#) (see page 191).

6. Verify that a system data source name (DSN) exists for the mode you specified. To do so, use the Data Sources (ODBC) Administrator option on the Windows Control Panel, as follows:
 - If necessary, create the system DSN.
Note: For instructions, see your Windows documentation.
 - If you are using 32-bit mode, verify that a system DSN exists for the 32-bit Data Source Administrator.
Note: The typical location of the 32-bit Data Source Administrator on a 64-bit operating system is C:\Windows\SysWOW64\odbcad32.exe.
 - If you are using 64-bit mode, verify that a system DSN exists for the 64-bit Data Source Administrator.
7. Start the CA Service Catalog Windows services.

You have configured components to run in 64-bit or 32-bit mode.

Updates Made by the Ant Command

You can optionally run the ant command to [configure components to run in 64-bit or 32-bit mode](#) (see page 189). For each CA Service Catalog product or component installed locally, running this ant command does the following:

- Uninstalls the existing Windows services
- Installs new Windows services to run in the new mode you specified (32-bit or 64-bit), for the required Tanuki wrapper, JRE, and license files

If installed locally, each of the following CA Service Catalog services is affected:

- CA Service View
- CA Service Accounting
- CA Service Fulfillment
- CA Service Repository Agent
- Message Queue 4.1 Broker

Note: CA Service Catalog batch files always use the 32-bit JRE and therefore always run in 32-bit mode. This condition exists regardless of whether the Windows services for CA Service Catalog are running in 32-bit mode or 64-bit mode. In contrast, the Message Queue 4.1 Broker always runs in 32-bit mode. However, switching the broker to 64-bit mode configures the broker to use the 64-bit JRE instead of the 32-bit JRE.

Chapter 9: Maintenance

This section contains the following topics:

- [Files to Back Up Regularly](#) (see page 193)
- [CA Management Database](#) (see page 194)
- [Update the Password of the Database User](#) (see page 194)
- [Update the Database Host, Port, Instance, or Service Names](#) (see page 196)
- [Update the CA EEM Host Name and Application Names](#) (see page 198)
- [Update the Host Name and Port Number for Service View and CA Workflow](#) (see page 202)
- [How to Maintain Log Files](#) (see page 204)

Files to Back Up Regularly

Several CA Service Catalog files are updated during use. Back up these files regularly, using the following table as a guide. This table identifies the features that use files on the Service View server and their locations:

Feature	Folder
Request Attachments	%USM_HOME%\filestore\documents\requests
CA Service Catalog Images for services	%USM_HOME%\filestore\images\offerings
Documents	%USM_HOME%\filestore\documents
CA Service Catalog Forms	%USM_HOME%\filestore\forms
Data Objects and Data Views	%USM_HOME%\filestore\reporting
Offline Data Objects and Data Views	%USM_HOME%\filestore\reporting\offline
Custom files for CA Service Catalog, including custom images, data fields for business units, accounts and users. You can optionally store these files in a filestore (see page 187).	%USM_HOME%\filestore\custom. For example, suppose you customized data fields for business units, accounts and users. A sample folder name is %USM_HOME%\filestore\custom\locale\icusen (for English). Another example follows: Suppose you customized images for service option groups. In that case, a sample folder name is %USM_HOME%\filestore\custom\images\rateplans.
Data Mediation	%USM_HOME%\filestore\DataMediation

CA Service Repository Agent files (also known as Data Mediation Data Repository Agent)	%USM_HOME%\repagent. This folder contains these sub folders: \conf, \log, and \data.
----------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------

CA Management Database

CA product suites are integrated through a common enterprise data repository: the CA Management Database (MDB). The MDB provides a unified database schema for the management data stored by all CA products (mainframe and distributed).

CA products include an MDB running on one of several major database management systems. The MDB helps enable integration between CA products for managing your IT infrastructure.

Note: For additional information regarding MDB and maintenance strategies, see the MDB documentation included with your CA Service Catalog installation media.

Update the Password of the Database User

You can run the update-db-user command to change the password of the database user, to comply with security, governance, or other requirements. CA Service Catalog components use the logon credentials (user name and password) of the database user to access the database. The update-db-user command updates these password references globally to help ensure that CA Service Catalog continues to run efficiently throughout your environment. You run the update-db-user command on *every* computer in your environment that has a CA Service Catalog component installed.

To update the password of the database user

1. Use the Windows Control Panel, stop these services: CA Service View, CA Service Accounting, CA Service Fulfillment, and Message Queue 4.1 Broker.

Important! Stop these services on *all* CA Service Catalog computers in your environment before proceeding to the next step! First, stop the services on all computers. Next, perform the following steps, on each CA Service Catalog computer, one at a time, until you have run the update-db-user command on all of them.

Note: If you are using vertical clustering, you do *not* need to run the command on every vertical cluster individually. Instead, run command only *once* on the computer where the verticals clusters are configured.

2. Open the CA Service Catalog command prompt by clicking Start, Programs, CA, Service Catalog, Service Catalog Command Prompt.

3. At the CA Service Catalog command prompt, enter the following command:

```
ant update-db-user
```

Note: For a list of ant commands and their descriptions, enter `ant -p`.

- a. Follow the prompts to update the password.

Your new or updated password is echoed in plain text but is saved in encrypted format.

- b. Confirm that you typed the password exactly as you intended, *including* the case.

Important! The password can be case-sensitive, depending on whether your DBMS is configured as case-sensitive. If necessary, see your DBMS administrator or DBMS documentation for details.

- c. If necessary, do the following:

- Correct any errors by canceling the `ant update-db-user` command and rerunning it.
- Record the password in a safe location for reference.

The command utility does the following:

- Backs up the existing versions of the `pm.xml`, `wl.xml`, `DBSource.properties`, and other configuration files
- Updates the logon credentials of the database user in these configuration files
- Updates the logon credentials in your DBMS (Oracle or SQL Server)
- Records the actions it performs in the `maintenance.log` file

This log file and the backed up configuration files are stored in the `%USM_HOME%\conf-backup\date-time` folder. The name of the `\date-time` subfolder is based on the date and time at which the `ant update-db-user` command was run. Thus, this subfolder name is different on each computer in the environment. The utility writes the name of the subfolder to the screen as soon as the backup is completed.

4. Do the following:
 - a. View the `maintenance.log` file in the `%USM_HOME%\conf-backup\date-time` folder for a record of the actions performed.
 - b. Record the name of this folder for future reference.
5. When you have finished running the command on the current computer, run it on the next computer, using the previous steps as a reference.

Note: Before you proceed to the next step, verify that you have run the command on *all* CA Service Catalog computers.

6. On every CA Service Catalog computer, restart the CA Service Catalog services that you shut down previously.
7. Verify that CA Service Catalog is running correctly, as follows:
 - a. Log in to CA Service Catalog.
 - b. Create services, create and process requests, and perform administrative tasks.

You can also run the `update-db-user` command to [update the database host, port, instance, or service names](#) (see page 196) or to [migrate](#) (see page 75).

Update the Database Host, Port, Instance, or Service Names

To comply with changes in your environment or for other reasons, you can change any or all of the following database settings: host name, port number, instance name, or service name. CA Service Catalog components use these settings to communicate with each other and the database.

To update the database host name, port number, instance name, or service name

1. Perform the following prerequisite tasks:
 - a. If you need to update the database host name, update the operating system computer name of the computer on which the database is installed. For details, see your operating system documentation.
 - b. Update these database settings in your DBMS software (Oracle or SQL Server). For details, see your DBMS documentation.
 - c. Verify that the updated DBMS is accessible from every DBMS client on every CA Service Catalog computer. Use your DBMS client software (not CA Service Catalog) to perform this step.

Note: If you are using vertical clustering, you do *not* need to update the database settings on every vertical cluster node individually; instead, you need to update the database settings only *once* on the computer where the vertical cluster nodes are configured.

- d. Using the Windows Control Panel, stop these services: CA Service View, CA Service Accounting, CA Service Fulfillment, and Message Queue 4.1 Broker.

Important! Stop these services on *all* CA Service Catalog computers in your environment before proceeding to the next step! After stopping the services on all computers, perform the steps that follow, on each CA Service Catalog computer, one at a time, until you have updated the database settings on all of them.

2. Open the CA Service Catalog command prompt by clicking Start, Programs, CA, Service Catalog, Service Catalog Command Prompt.

The command prompt opens.

3. [Run the ant update-db-user command](#) (see page 194), if *both* of the following conditions exist. Otherwise, skip this step.

- You are using SQL Server
- The database was backed up and restored on a new computer

The ant update-db-user command updates the password of the database user.

When you are prompted for your password, optionally specify your existing password if you want to continue using it.

4. Enter the following command at the CA Service Catalog command prompt:

```
ant update-db-host
```

Note: For a list of ant commands and their descriptions, enter ant -p.

The utility displays the current settings for the database host name, port number, and either instance name (for SQL Server), or service name (for Oracle).

You are prompted to accept or change each setting.

5. Follow the prompts to update each setting that you want to change, and confirm the new value.

- If you are using SQL Server, if applicable, update the instance name for the MDB. For example, myinstance. The default value is MSSQLSERVER.

Important! Instances must reside on a static port!

- If you are using Oracle, if applicable, update the service name; every Oracle database or service has a service name. The service name of an Oracle database is typically its global database name. Enter the service name of the Oracle database or other service that you want to access.

If necessary, to correct any errors, cancel and re-run the ant update-db-host command.

6. Record all updated database settings for reference.

The command utility does the following:

- Backs up the existing versions of the pm.xml, wl.xml, DBSource.properties, and other configuration files
- Updates the following settings in these configuration files: host name, port number, instance name, or service name
- Updates the same settings in your DBMS (Oracle or SQL Server)
- Records the actions it performs in the maintenance.log file

This log file and the backed up configuration files are stored in the %USM_HOME%\conf-backup*date-time* folder. The name of the *date-time* subfolder is based on the date and time at which the ant update-db-host command was run. Thus, this subfolder name is different on each computer in the environment. The utility writes the name of the subfolder to the screen as soon as the backup is completed.

7. Do the following:
 - a. View the maintenance.log file in the %USM_HOME%\conf-backup*date-time* folder for a record of the actions performed.
 - b. Record the name of this folder for future reference.

Note: Before proceeding to the next step, verify that you have run ant update-db-host command on *all* CA Service Catalog computers.
8. On every CA Service Catalog computer, restart the CA Service Catalog services that you shut down previously.
9. Verify that CA Service Catalog is running correctly, as follows:
 - a. Log in to CA Service Catalog.
 - b. Create services, create and process requests, and perform administrative tasks.

The new or updated database settings are updated in the Windows registry. As a best practice, back up the Windows registry after you update the database settings; for details, see your Windows documentation.

Update the CA EEM Host Name and Application Names

To comply with security, governance, or other requirements, you can change the name of the host computer running CA EEM. You can also change the names of the applications whose access control you manage through CA EEM. These applications can be one or more CA products, such as CA Service Desk Manager, CA CMDB, CA Service Catalog, and so forth. To change these names, you run the update-eem-host command utility on *every* computer in your environment that has a CA Service Catalog component installed. This utility updates these names globally. Doing so helps ensure that CA Service Catalog, CA EEM, and their integrated products continue to run efficiently throughout your environment

Note: In this topic, the term *application names* refers to the CA EEM policies for managing access control for users and other resources to these products. Thus, in CA EEM, the application name *Service Delivery* refers to the policies governing user access control in CA Service Catalog. CA EEM also includes a *Global* application name that you can optionally apply in part or in whole to one or more products. For details about integrating CA Service Catalog and CA EEM, see the *Integration Guide*.

To update the CA EEM host name and application names

1. Open the CA Service Catalog command prompt by clicking Start, Programs, CA, Service Catalog, Service Catalog Command Prompt.
2. Verify that both the old and new CA EEM host computers are running if you are changing computers. Otherwise, skip to the next step.

3. Run the following command at the CA Service Catalog command prompt *before* changing the computer name. If you are changing only the computer *name*. Otherwise, skip to the next step.

```
ant backup-eem-app
```

This action generates a file named eem-backup.xml in the %USM_HOME% directory.

4. Perform this step if you want to change the name of the CA EEM computer. Otherwise, skip to the next step. For example, if you are moving CA EEM from one computer to another, skip to the next step.
 - a. Change the computer name.
 - b. Reboot the computer.
 - c. Update the CA EEM configuration with the new computer name, according to the instructions in the CA EEM documentation.
5. Use the Windows Control Panel to stop these services: CA Service View, CA Service Accounting, CA Service Fulfillment, and Message Queue 4.1 Broker.

Important! Stop these services on *all* CA Service Catalog computers in your environment before proceeding to the next step! Stop the services on all computers. Next, perform the steps that follow, on each CA Service Catalog computer, one at a time, until you have updated the CA EEM host name and application names on all of them.

Note: If you are using vertical clustering, you do *not* need to update the CA EEM host name and application names on every vertical cluster individually. Instead, update these names only *once* on the computer where the verticals clusters are configured.

6. Perform this step if you have an existing backup file. Otherwise, skip to the next step.
 - a. Copy the backup file to the %USM_HOME% directory and rename it to eem-backup.xml.
 - b. Enter the following command at the CA Service Catalog command prompt:

```
ant update-eem-host -Duse.existing.eem.backup=true
```

Note: For a list of ant commands and their descriptions, enter ant -p.

7. Enter the following command if you do *not* have an existing backup file. Otherwise, skip to the next step.

```
ant update-eem-host
```

- a. Follow the prompts to update the CA EEM host name and application names.
If the name that you specify is new, the command utility creates the name in the CA EEM database.
The new or updated names are echoed.
- b. Confirm that you entered the new name exactly as you intended, *including* the case. Correct the name if necessary.
Important! The new names can be case-sensitive, depending on whether your DBMS is configured as case-sensitive. If necessary, see your DBMS administrator or DBMS documentation for details.
- c. If necessary, to correct any errors, cancel and rerun the ant update-eem-host command.
- d. Record the new names in a safe location for reference.

The command utility does the following:

- Backs up the existing versions of the pm.xml, wl.xml, EIAM.properties, and other configuration files
- Updates the host name and application names in these configuration files
- Updates the host name and application names in your DBMS (Oracle or SQL Server)
- Records the actions it performs in the maintenance.log file

This log file and the backed up configuration files are stored in the %USM_HOME%\conf-backup*date-time* folder. The name of the *date-time* subfolder is based on the date and time at which the ant update-eem-host command was run. Thus, this subfolder name is different on each computer in the environment. The utility writes the name of the subfolder to the screen as soon as the backup is completed.

8. Do the following:
 - a. View the maintenance.log file in the %USM_HOME%\conf-backup*date-time* folder for a record of the actions performed.
 - b. Record the name of this folder for future reference.

Note: Before you proceed to the next step, verify that you have updated the host name and application names on *all* CA Service Catalog computers.
9. On every CA Service Catalog computer, restart the CA Service Catalog services that you shut down previously. Verify that CA Service Catalog is running correctly, as follows:
 - a. Log in to CA Service Catalog.
 - b. Create services, create and process requests, and perform administrative tasks.

The new or updated host name and application names are updated in the Windows registry.

Note: As a best practice, back up the Windows registry after you update the host name and application names. For details, see your Windows documentation.

Update the Host Name and Port Number for Service View and CA Workflow

You can change the host name, port number, or both for a computer running Service View, CA Workflow, or both. You can do so to adapt to changes in your environment or for other reasons. CA Service Catalog use these settings to communicate with other components, the database, and other CA products. You perform these steps *only* on the computer whose host name or port number has changed. You do not perform these steps on *other* computers.

Note: If applicable, you use the operating system (not the `ant update-usm-host` command) to change the host name. Afterwards, you use the `ant` command to propagate that host name change throughout the catalog system. However, you use the `ant` command to both update the port number directly *and* propagate that change throughout the catalog system.

To update the host name and port number for Service View and CA Workflow

1. Use the operating system to update the computer name (host name) of the computer on which Service View is installed, if necessary.

Note: For details, see your operating system documentation.

Use the Windows Control Panel to stop these services on the computer being updated: CA Service View, CA Service Accounting, CA Service Fulfillment, and Message Queue 4.1 Broker.

Important! Stop these services on *all* CA Service Catalog computers in your environment *before* proceeding to the next step! After you stop the services on all computers, perform the steps that follow.

Note: If you are using vertical clustering, you do *not* need to update the computer name on every vertical cluster node individually. Instead, update the computer name only *once* on the computer where the vertical cluster nodes are configured.

2. Do the following:

- a. Open the CA Service Catalog command prompt by clicking Start, Programs, CA, Service Catalog, Service Catalog Command Prompt.

The command prompt opens.

- b. Enter the following command at the CA Service Catalog command prompt:

```
ant update-usm-host
```

Note: For a list of ant commands and their descriptions, enter `ant -p`.

The utility displays the current settings for the host name and port number.

You are prompted to accept or change the port numbers.

- c. Follow the prompts to update each setting that you want to change, and confirm the new value.

If necessary, to correct any errors, cancel and rerun the `ant update-usm-host` command.

- d. Record all updated host name and port number settings for reference.

The command utility does the following:

- Backs up the existing versions of the `pm.xml`, `wl.xml`, `DBSource.properties`, and other configuration files
- Updates the host name and port number settings in these configuration files
- Updates the host name and port number settings in your DBMS (Oracle or SQL Server)
- Records the actions it performs in the `maintenance.log` file

This log file and the backed up configuration files are stored in the `%USM_HOME%\conf-backup\date-time` folder. The name of the `date-time` subfolder is based on the date and time at which the `ant update-usm-host` command was run. Thus, this subfolder name is different on each computer in the environment. The utility writes the name of the subfolder to the screen as soon as the backup is completed.

3. Do the following:

- a. View the `maintenance.log` file in the `%USM_HOME%\conf-backup\date-time` folder for a record of the actions performed.

- b. Record the name of this folder for future reference.

4. Verify that you have finished updating the host name and port number on the current computer. Update the host name and port number on the next computer, if necessary.

Note: Before you proceed to the next step, verify that you have updated the required settings on *all* CA Service Catalog computers.

5. Log in to CA Service Catalog.
6. Perform this step *only* if you are using CA Workflow *and* you updated the host name or port number of CA Workflow. Otherwise, skip this step.

Set the [CA Workflow configuration parameters](#) (see page 121) and update the CA Workflow actors.

7. Perform this step *only* if you are upgrading from a previous release *and* you are using CA Workflow. If you are installing CA Service Catalog for the first time *or* if you are not using CA Workflow, skip this step.

Do *one* of the following if you updated the host name or port number of Service View and you are using *custom* CA Workflow process definitions. If you are using the predefined CA Workflow process definitions, this step is not required.

- Enable the CA Service Catalog process definitions.

Note: For details about enabling process definitions, see the *Integration Guide*.

- Export, update, and import the existing process definitions, as follows:

- a. Export the process definitions in CA Workflow.
- b. Use a file editor to open the XML file of each exported process definition. In that file, replace the old host name for Service View with the new host name.
- c. Import the updated process definitions in CA Workflow.

The updated process definitions are enabled.

8. Verify that CA Service Catalog is running correctly, as follows:
 - a. Log in to CA Service Catalog.
 - b. Create services, create and process requests, and perform administrative tasks.

The new or updated host name and application names are updated in the Windows registry.

Note: As a best practice, back up the Windows registry after you update the database settings. For details, see your Windows documentation.

How to Maintain Log Files

CA Service Catalog includes nearly approximately 50 log files, each of which is helpful for researching a specific component, function, or question. To maintain log files, do the following:

1. Review the [names and locations of all log files](#) (see page 205).
2. Review the descriptions of the [most frequently used log files](#) (see page 207).

3. Become familiar with the process of [setting log levels](#) (see page 210).
4. Review the process of [configuring rollover settings for selected log files](#) (see page 213).
5. To keep older rolled over log files from consuming excessive disk space, delete them manually at regular intervals.

Verify that you comply with the file retention policy of your organization. By default, certain log files are automatically rolled over and are automatically deleted periodically. Both processes occur according to your specifications when you [configure rollover settings for selected log files](#) (see page 213). However, *no other* rolled over log files are automatically deleted; therefore, delete them manually.

Names and Locations of All Log Files

Most CA Service Catalog log files are located in the folder named %USM_HOME%\logs, as follows:

- The log file folder for Service View messages is %USM_HOME%\logs\view.
- The log file folder for installation messages is %USM_HOME%\logs\install.
- The log file folder for CA Workflow messages is %USM_HOME%\logs\fulfillment.
- The log file folder for CA Service Accounting messages is %USM_HOME%\logs\accounting.

The names and locations of *all* CA Service Catalog log files follow. This list includes the [most frequently used log files](#) (see page 207).

%USM_HOME%\logs

The following log files are located in %USM_HOME%\logs folder:

- view.log
- view.log.1, view.log.2, view.log.3, and so forth

You can [configure rollover settings for these log files](#) (see page 213).

%USM_HOME%\logs\accounting

The following log files are located in the %USM_HOME%\logs\accounting folder:

- accounting.log
- AccountingService.log

%USM_HOME%\logs\fulfillment

The following log files are located in the %USM_HOME%\logs\fulfillment folder:

- FulfillmentService.log
- pm.log
- pm.log.1, pm.log.2, pm.log.3, and so forth

You can [configure rollover settings for these log files](#) (see page 213).

- tomcat_fulfillment.log
- wf_admin.log
- wf_process.log
- wf_security.log
- wl.log
- wl.log.1, wl.log.2, wl.log.3, and so forth

You can [configure rollover settings for these log files](#) (see page 213).

- wsactorSoapRequest.xml
- wsactorSoapResponse.xml

%USM_HOME%\logs\install

The following log files are located in the %USM_HOME%\logs\install folder:

- acnt_seed_data.log
- createFiscalPeriod.log
- createRootOffering.log
- DeployServices.log
- importCommonReports.log
- importPlanningContent.log
- importPortalContent.log
- imq_cfg1.log
- imq_cfg2.log
- imq_cfg3.log
- InstallProducts.log
- ixerr.log
- ixutil.log

- seeddata.log
- sqlUtil.log
- usm_eiam_check.log
- usm_eiam_viewG.log
- usm_eiam_viewL.log
- usmInstall.log
- view_seed_data.log
- wf_seed_data.log
- workflow_install.log

%USM_HOME%\logs\view

The following log file is located in the %USM_HOME%\logs\view folder:

- postEvent.log
- tomcat_view.log
- ViewService.log

%USM_HOME%\logs\repagent

The following log files are located in the %USM_HOME%\logs\repagent folder:

- repagent.log
- RepositoryAgentService.log

Most Frequently Used Log Files

This topic lists and describes the log files that you are likely to review most frequently. If a file is marked with an asterisk (*), you can [set the logging levels](#) (see page 210) for the file.

accounting.log*

Stores log messages generated by CA Service Accounting, but not by its Windows service.

This file located in the %USM_HOME%\logs\accounting folder.

AccountingService.log

Stores log messages generated by the Windows service of CA Service Accounting.

This file located in the %USM_HOME%\logs\accounting folder.

ixutil.log*

Stores log messages generated by the ixutil import/export command line utility.
This file located in the %USM_HOME%\logs folder.

repagent.log*

Stores log messages generated by the CA repository agent.
This file located in the %USM_HOME%\logs\repagent folder.

RepositoryAgentService.log

Stores log messages generated by the Windows service of the repository agent.
This file located in the %USM_HOME%\logs\repagent folder.

seeddata.log*

Stores log messages generated when the database is seeded with the initial data supplied with CA Service Catalog to get it started and running immediately after installation.
This file located in the %USM_HOME%\logs folder.

view.log*, view.log.1*, view.log.2*, view.log.3* and so forth

Store log messages generated by the Service View component, including [rolled over log files](#) (see page 213) from previous days.
These files are located in the %USM_HOME%\logs folder.

ViewService.log

Stores log messages generated by the Windows service of Service View.
This file located in the %USM_HOME%\logs\view folder.

pm.log, pm.log.1, pm.log.2, pm.log.3, and so forth

Store log messages generated by the Process Manager component of CA Workflow, including [rolled over log files](#) (see page 213) from previous days.
These files are located in the %USM_HOME%\logs\fulfillment folder.

tomcat_fulfillment.log*

Stores log messages generated by Apache Tomcat hosting the CA Service Fulfillment service.
This file located in the %USM_HOME%\logs\fulfillment folder.

wl.log, wl.log.1, wl.log.2, wl.log.3, and so forth

Stores log messages generated by the Worklist Manager component of CA Workflow, including [rolled over log files](#) (see page 213) from previous days.

These files are located in the %USM_HOME%\logs\fulfillment folder.

usmInstall.log

Stores log messages generated by the CA Service Catalog uninstallation program.

This file located in the %USM_HOME%\logs\install folder.

tomcat_view.log*

Stores log messages generated by Apache Tomcat hosting Service View and CA Service Accounting services.

This file located in the %USM_HOME%\logs\view folder.

How to Set Log Levels

You can set the logging levels (the level of detail) for some of the [most frequently used log files](#) (see page 207) in CA Service Catalog, using the Apache Tomcat log4j file. Configuring the log level helps you better maintain your log files and troubleshoot any problems that occur in your system.

Note: CA Workflow creates the log files named wl.log and pm.log. For instructions on how configure their output, see the *CA Workflow IDE Online Help*. The logging levels for *all other* log files supplied by CA Service Catalog are preset and cannot be modified.

To set logging levels for the files named in the previous list, follow this process:

1. From the following list, determine the log file whose output you want to control. If necessary, review the contents of each file. These files are some of the most frequently used log files in CA Service Catalog.
 - accounting.log
 - ixutil.log
 - repagent.log
 - seeddata.log
 - tomcat_fulfillment.log
 - tomcat_view.log
 - view.log
2. Determine the [log4j.xml file](#) (see page 211) that controls the output of the log file whose log level you want to set.
3. Edit that log4j file and [set the new logging level](#) (see page 212).
4. After sufficient time has passed (approximately 60 seconds), review the contents of the affected log file. Verify whether the level of detail of its messages is satisfactory. If necessary, reset the log level and review the contents again until you are satisfied with the level of detail.
5. As appropriate, consult other administrators to see if the level of detail logged meets their needs.

Note: For additional information about the logging features that CA Service Catalog uses, see the information about log4j on <http://jakarta.apache.org>.

Log Files Controlled by Each Log4j.xml File

CA Service Catalog includes several log4j.xml files that control the output of the [most frequently used log files](#) (see page 207). Each log4j.xml file controls the log file of one or more CA Service Catalog services, as summarized in the following table:

Service Logged	Location of Log4j File	Log Files Controlled	Log file Location
Service View	%USM_HOME%\view\conf	seeddata.log view.log tomcat_view.log	%USM_HOME%\logs\install %USM_HOME%\logs %USM_HOME%\logs\view
CA Service Fulfillment	%USM_HOME%\fulfillment\conf	tomcat_fulfillment.log	%USM_HOME%\logs\fulfillment
CA Service Accounting	%USM_HOME%\accounting\conf	accounting.log	%USM_HOME%\logs\accounting
Repository Agent	%USM_HOME%\repository\config	repagent.log	%USM_HOME%\repository\log
ixutil import\export utility	%USM_HOME%\scripts	ixutil.log	%USM_HOME%\logs\install

Logging messages generated by CA Service Catalog components, such as the Event Manager and the Rule Engine, are written to the log file of the calling service. For example, if the Service View service calls the Event Manager, the log for the call is written in the view.log file. Similarly, calls from the CA Service Accounting service to the Event Manager are written to the accounting.log file.

Set the Log Level of a Service

You can change the log level of a CA Service Catalog service for various reasons. For example, you can set the log level to a higher level to investigate a problem or question. After you are finished investigating, you can reduce the log level for efficiency reasons.

To set the log level of a service

1. Open the [log4j.xml file](#) (see page 211) of the CA Service Catalog service whose logging level you want to set.
2. Find the following section:

```
<root>
<priority value="log-level" />
<appender-ref ref="accounting" />
<!-- appender-ref ref="console" /-->
</root>
```

3. Specify one of the following for the *log-level*:

Fatal

Logs only errors that shut down a CA Service Catalog component. This log level typically provides the least detail. It also requires the least amount of disk space for rolled-over log files and therefore the least maintenance.

Error

Logs all of the messages from the previous level, plus failed actions. For example, a user submitted a request, but the system did not present the request for approval.

Warn

Logs all of the messages from the previous levels, plus warning messages; for example, a user creates a service with a nonunique name.

Informational

Logs all of the messages from the previous levels, plus messages that are informational only. An example is the total number of open database connections.

Debug

Logs all of the messages from the previous levels, plus more detailed messages intended to help troubleshoot a problem. For example, debug messages can include every step of a multiple-step process.

Trace

Logs every action and displays the final XML. This level includes all of the messages from the previous levels, plus many more.

This log level typically provides the most detail. It also requires the most amount of disk space for rolled-over log files and therefore the most maintenance.

4. Save and close the log4j.xml file.
5. Recycle the CA Service Catalog service whose logging level you updated.

Important! Do *not* make any *other* changes to any log4j file, unless instruction to do so by CA Technical Support!

Configure Rollover Settings for Selected Log Files

To maintain maximum efficiency, CA Service Catalog automatically rolls over selected frequently used log files, according to default settings. For any of these log files, you can configure both the rollover size and the number of rolled over log files retained. Doing so helps you customize the log files to match the needs of your organization more closely.

To configure rollover settings for selected log files

1. Review the selected frequently used log files that you can edit, including the default rollover settings. Decide the file that you want to update.
2. Open the [log4j.xml file](#) (see page 211) that controls the output for the log file that you want to update. Use an editor of your choice. (see page 211)
3. Find the following section:

```
<appender name="view" class="org.apache.log4j.RollingFileAppender">
  <param name="File" value="{usm.home}/logs/view.log" />
  <param name="MaxFileSize" value="size" />
  <Param name="MaxBackupIndex" value="backup-index" />
  ...
</appender>
```

4. Specify the following settings:

size

Specifies the rollover size; that is, the file size at which you want this log file to roll over, in MB. For example, enter 5 to make the log file roll over when its size reaches 5 MB.

Default: 10

backup-index

Specifies the number of recently rolled over log files that you want to keep on disk, for example, 25 or 50.

Default: 100

5. Save and close the log4j.xml file.
6. After one or more days have passed, verify that the log file output matches your needs. If necessary, reconfigure the log4j file or files to match your needs more closely.

You have configured the rollover settings for selected log files.

Chapter 10: Clustering

This section contains the following topics:

- [How to Implement Clustering](#) (see page 215)
- [Perform the Preliminary Tasks](#) (see page 216)
- [Meet the Prerequisites](#) (see page 217)
- [How to Set Up Vertical Clustering for Service View](#) (see page 218)
- [Set Up Horizontal Clustering for Service View](#) (see page 228)
- [Set Up NTLM Authentication for Each Cluster](#) (see page 230)
- [Set Up Horizontal Clustering for CA Workflow](#) (see page 233)
- [How to Set Up Load Balancing](#) (see page 236)

How to Implement Clustering

As a CA Service Catalog administrator, you can optionally use *clustering* for CA Workflow and Service View to improve performance and provide *failover protection*. Here, the term *clustering* means multiple computers grouped together performing the same or similar function, essentially acting as one virtual computer. Specifically, clustering here refers to CA Workflow and Service View running on two or more computers. *Failover protection* means that if one computer malfunctions, becomes heavily loaded, or loses power, its workload is transferred to the other computers in the cluster. These computers retain and complete the active sessions.

Another advantage of clustering is *load-balancing*: If one of the cluster components is busy processing a request, the load is redirected to another component in the cluster. Users of the system see no interruption of access. CA Workflow and Service View processing for CA Service Catalog continues. The loss of performance on users and business functions is minimized, even when computer availability is lost or reduced.

To implement clustering for CA Workflow and Service View, perform these tasks:

1. [Perform the preliminary tasks](#) (see page 216).
2. [Meet the prerequisites](#) (see page 217).
3. To implement clustering for Service View, do one or both of the following:
 - [Set up vertical clustering for Service View](#) (see page 218)
 - [Set Up horizontal clustering for Service View](#) (see page 228)
4. [Set up NTLM authentication for each cluster](#) (see page 230), if applicable.
5. [Configure NTLM with Apache Load Balancer](#) (see page 231), if applicable.
6. Optionally [set up horizontal clustering for CA Workflow](#) (see page 233).

7. [Set up load balancing](#) (see page 236).
8. If you are implementing horizontal clustering on multiple computers, use the computers that have the same default gateway. To obtain the default gateway, enter the ipconfig command at the DOS prompt.

Also, consider [setting up a single location for shared files](#) (see page 187). While this task is not directly related to clustering, it does help improve overall system performance and helps reinforce best practices.

Perform the Preliminary Tasks

Perform the following preliminary tasks before you [implement clustering](#) (see page 215):

1. Verify that you have installed CA Service Catalog, including Service View and CA Workflow.

The original installations of Service View and CA Workflow are used as building blocks for the additional cluster nodes.
2. Understand the [key terms and concepts](#) (see page 14) of clustering.
3. Decide whether to implement clustering for Service View, CA Workflow, or both. You can optionally implement clustering for only one, both, or neither.
4. For Service View, decide whether to use horizontal (multiple computer) clustering or vertical (same-computer) clustering.
5. Decide whether to set up horizontal clustering for CA Workflow; vertical clustering does *not* apply.
 - To implement horizontal clustering, you make several related configuration changes *manually*.
 - To implement vertical clustering, you do the following:
 - Specify the port numbers and cluster number of the node to create in the cluster.properties file.
 - Run the ant command that makes several related configuration changes *automatically*. This command uses your specifications from the cluster.properties file.
6. For Service View, CA Workflow, or both, decide how many cluster nodes to create, depending on your design concerns and availability of resources.
7. Verify that the time and time zone on all clustered computers are the same.
8. Verify that the IPV6 protocol is disabled on all clustered computers.

You have completed the preliminary tasks. Now you can [meet the prerequisites](#) (see page 217).

Meet the Prerequisites

To implement clustering successfully, meet its prerequisites.

To meet the prerequisites

1. Verify that no other application uses the following ports.

By default, CA Service Catalog uses these ports for clustering, using the AJP protocol:

- 8009 – for Service View communicating with Apache HTTP Server
- 8019 – Service Fulfillment communicating with Apache HTTP server

2. Perform this step if applicable; otherwise, skip it.

If another application uses one of these port numbers, eliminate the duplication by using a different port number for either CA Service Catalog or the other application.

If you use a different port number for CA Service Catalog, then also replace the old port number with the new port number in the applicable clustering topics in this documentation. For example, if you change 8009 to a different port number, use the new port number instead of 8009 when you [set up horizontal clustering for Service View](#) (see page 228).

3. Locate and record the multicast address in the server.xml file.

This address is the value of the mcastAddr attribute within the Membership tag. This value is typically 228.0.0.4, as shown in the following sample specification:

```
<Membership className="org.apache.catalina.cluster.mcast.McastService" mcastAddr="228.0.0.4" mcastPort="45564" mcastFrequency="500" mcastDropTime="3000" />
```

4. Verify that each clustered computer can ping this multicast address.

If each clustered computer can ping the multicast address, then skip rest of the steps in this topic. If not, then complete the remaining steps.

5. Run the following command at the DOS prompt of each clustered computer:

```
netsh interface ip show joins
```

The system displays all the multicast addresses that this computer can ping.

6. Determine a common multicast address that all clustered computers can ping.

7. Update the mcastAddr value in the server.xml file on all clustered computers to use the common multicast address that you determined in the previous step.

Note: Update this file on all clustered computers before proceeding to the next step.

8. Restart the CA Service Catalog Windows service on all clustered computers.
9. Optional) Repeat the previous steps to set up a second environment, if applicable.

Note: If you use the same multicast address for both environments, use a different multicast port number for each environment.

You have met the prerequisites.

How to Set Up Vertical Clustering for Service View

To set up vertical clustering for Service View, perform these tasks:

1. [Perform the initial setup](#) (see page 219).
The original installation is your first cluster.
2. [Set up each additional cluster](#) (see page 220) that you want to create. You perform this procedure one to many times, once for each new cluster that you want to create.
3. Review the [updates made automatically](#) (see page 222) when you set up each cluster in the previous step.
4. [Verify the server.xml files](#) (see page 225).
5. If you are using NTLM authentication to enable single sign-on to CA Service Catalog, [set up NTLM authentication for each cluster](#) (see page 230); otherwise, skip this step.
6. After you set up all Service View clusters, [set up load balancing](#) (see page 236).

Perform the Initial Setup

This procedure is required to set up vertical clustering for Service View. You perform this procedure only once. The original installation is your first cluster.

Note: Before you perform this procedure, verify that Service View is installed locally.

To perform the initial setup

1. On the computer with the original Service View installation, open the %USM_HOME%\view\conf\server.xml file for editing.
2. Uncomment the Cluster tags shown in the following lines, if they are commented:

```
<Cluster className="org.apache.catalina.cluster.tcp.SimpleTcpCluster"
  managerClassName="org.apache.catalina.cluster.session.DeltaManager"
  expireSessionsOnShutdown="false"
  useDirtyFlag="true" notifyListenersOnReplication="true">

  <Membership className="org.apache.catalina.cluster.mcast.McastService"
mcastAddr="228.0.0.4" mcastPort="45564"
  mcastFrequency="500" mcastDropTime="3000" />

  <Receiver className="org.apache.catalina.cluster.tcp.ReplicationListener"
tcpListenAddress="auto"
  tcpListenPort="4001" tcpSelectorTimeout="100" tcpThreadCount="6" />

  <Sender className="org.apache.catalina.cluster.tcp.ReplicationTransmitter"
replicationMode="pooled"
  ackTimeout="15000" />

  <Valve className="org.apache.catalina.cluster.tcp.ReplicationValve"
filter=".*\.(gif|\.js|\.jpg|\.png|\.css|\.txt);" />

  <Deployer className="org.apache.catalina.cluster.deploy.FarmWarDeployer"
tempDir="/tmp/war-temp"
  deployDir="/tmp/war-deploy/" watchDir="/tmp/war-listen/" watchEnabled="false" />

  <ClusterListener className="org.apache.catalina.cluster.session.ClusterSessionListener" />

</Cluster >
```

3. Uncomment the Apache JServ Protocol (AJP) tags shown in the following lines, if they are commented:

```
<Connector port="8009" maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" redirectPort="8443" protocol="AJP/1.3" />
```

4. Save the file.

5. Restart the CA Service View service.
6. Review the tomcat_view.log file of each Service View component and verify that the replication cluster was added. For example:

```
INFO Cluster-MembershipReceiver org.apache.catalina.cluster.tcp.SimpleTcpCluster - Replication member added:
org.apache.catalina.cluster.mcast.McastMember[tcp://141.202.143.77:4013,catalina,141.202.143.77,4013,alive=0]
```

7. Copy the cluster.properties.example file located in the %USM_HOME% directory to a new file named cluster.properties.

You have performed the initial setup.

Set Up Each Additional Cluster

This procedure is required to set up vertical clustering for Service View. Perform this procedure once for *each* new cluster that you want to create in addition to the original installation. For example, to set up two new clusters in addition to the original installation, you perform this procedure twice. Each time you perform this procedure, you update the *same* cluster.properties file before you run the ant command.

To set up each additional cluster

1. Open the cluster.properties file for editing.
2. Modify the port numbers and the cluster number listed in the following parameters. Verify that each number is unique across all clusters.

The defaults listed in these parameters are the initial values for the first node created. For later nodes, increase this number so that it is unique. Ideally, increase the port and cluster numbers by 1 from the previous cluster.

Note: Consider running the Windows netstat command to help identify which ports are available.

view.node.id=number

Specifies the number of the cluster.

The default is 1.

view.shutdown.port=number

Specifies the Tomcat shutdown port for this node.

The default is 8086.

view.http.port=*number*

Specifies the Tomcat startup port for this node.

The default is 8081.

view.ajp.port=*number*

Specifies the ajp port for the load balancer to communicate with this node.

The default is 8010.

view.receiver.port=*number*

Specifies the Tomcat cluster receiver node.

The default is 4003.

3. Navigate to the %USM_HOME% folder in Windows Explorer and double-click the usm.cmd file.

The CA Service Catalog command prompt opens, with the location set to the %USM_HOME% folder path.

4. Run the following command at that prompt:

```
ant install-view-node
```

The ant command makes several [configuration changes and other updates](#) (see page 222).

5. (Optional) View the new log file to verify that the node has started without any exceptions.
6. (Optional) Verify that the node is functioning by using the URL `http://hostname:(view.http.port)/usm/wpf`.

You have set up additional clusters.

Updates Made Automatically When You Set Up a Cluster

When you run the ant command to [set up each additional cluster](#) (see page 220), it makes several updates to files and folders, as follows:

- Copies and creates files, folders, and services
- Updates the following files in the `Viewnumber\conf` folder with required changes:
 - [server.xml](#) (see page 222)
 - [viewservice.conf](#) (see page 224)
 - [log4j.properties](#) (see page 224)

Note: The *number* in *Viewnumber* specifies the node number of the cluster, which is also named the cluster number. For example, View1 is the folder for cluster 1, View2 is the folder for cluster 2, and so forth.

- Adds a [new Windows service](#) (see page 225), using the viewservice.bat file

Updates to the Server.xml File

Running the ant command to create a Service View cluster automatically makes the following changes to the server.xml file in the `Viewnumber\conf` folder. In the folder name, *number* specifies the cluster number.

- Updates server port in the following line with the view.shutdown.port number specified in the cluster.properties file. This port number must be unique.

```
<Server port="8085" shutdown="SHUTDOWN" debug="0">
```

- Updates the HTTP connector port in the following lines with the view.http.portnumber specified in the cluster.properties file. This port number must be unique.

```
<Connector port="8080" minProcessors="5" maxProcessors="200"  
enableLookups="true" redirectPort="8443"
```

- Updates the ajp connector port in the following lines with the view.ajp.port number specified in the cluster.properties file. This port number must be unique.

```
<Connector port="8009"  
enableLookups="false" redirectPort="8443" protocol="AJP/1.3"  
emptySessionPath="true" />
```

- Constructs the `jvmRoute` by appending the following strings:
 - `_hostname` specifies the computer name of the cluster.
 - `_usmViewnumber` or `_cawfnumber`. specifies the name and number of the service which is being clustered:

If the CA Service View service is being clustered, the string `usmviewnumber` is appended.

If the CA Service Fulfillment service is being clustered, the string `cawfnumber` is appended.
 - For both `usmviewnumber` and `cawfnumber`, `number` is the cluster number specified in the `view.id.node` parameter in the `cluster.properties` file. The first node of the cluster has no number; the second node is number 1, the third node is number 2, and so forth.

For example, if the CA Service View service is clustered on a host named XYZ, its `jvmroute` name is XYZ_usmview. If a vertical cluster is added to this node using the ant command, the `jvmroute` name is XYZ_usmview1. Additional vertical nodes are named XYZ_usmview2, XYZ_usmview3, and so forth.
- Uncomments the cluster tag, and updates the `tcplisten` port of receiver with the `view.receiver.port` number specified in the `cluster.properties` file. For example, see the following lines:

```
<Receiver  
    className="org.apache.catalina.cluster.tcp.ReplicationListener"  
    tcpListenAddress="auto"  
    tcpListenPort="4002"  
    tcpSelectorTimeout="100"  
    tcpThreadCount="6"/> <Receiver
```

Updates to the Viewservice.conf File

Running the ant command to create a Service View cluster automatically makes the following updates to the viewservice.conf file. This file is located in the *Viewnumber*\conf folder; in the folder name, *number* specifies the cluster node number.

- In each of the following lines, *number* specifies the cluster node number from the `view.node.id=number` parameter in the cluster.properties file:

```
wrapper.java.additional.15=-Dtomcat.home="%USM_HOME%/viewnumber"  
wrapper.java.additional.17=-Dlog4j.configuration="file:%USM_HOME%/viewnumber/conf/log4j.properties"  
wrapper.java.additional.21=-Dcatalina.base="%USM_HOME%/viewnumber"  
wrapper.logfile=././logs/ViewServicenumber.log  
wrapper.ntservice.name=ServiceViewnumber  
wrapper.ntservice.displayName=CA Service Viewnumber  
wrapper.ntservice.description=CA:CA Service Viewnumber
```

For example, if this cluster node is the first one being added to a Service View computer, then running the ant command creates a folder named View1\conf with a new viewservice.conf file. That file contains the following lines:

```
wrapper.java.additional.15=-Dtomcat.home="%USM_HOME%/view1"  
wrapper.java.additional.17=-Dlog4j.configuration="file:%USM_HOME%/view1/conf/log4j.properties"  
wrapper.java.additional.21=-Dcatalina.base="%USM_HOME%/view1"  
wrapper.logfile=././logs/ViewService1.log  
wrapper.ntservice.name=ServiceView1  
wrapper.ntservice.displayName=CA Service View1  
wrapper.ntservice.description=CA:CA Service View1
```

- For the jms client ID, *number* specifies the cluster number from the `view.node.id=number` parameter in the cluster.properties file. This line uses the following format:

```
wrapper.java.additional.9=-Djms.clientid=hostname_USMViewnumber
```

For example, if the host name is XYZ and this cluster is the first one, then this line is as follows:

```
wrapper.java.additional.9=-Djms.clientid=XYZ_USMView1
```

Updates to the Log4j.properties File

Running the ant command automatically makes the following change to the log4j.properties file in the *Viewnumber*\conf folder. In the folder name and in the following lines, *number* specifies the cluster number.

- Specifies the cluster number from the `view.node.id=number` parameter in the cluster.properties file:

```
Log4j.appender.R.File=${usm.home}/logs/view_logs/tomcat_viewnumber.log
```

For example, you can specify view1, view2, or view3.

New Windows Service

Running the ant command to create a Service View cluster automatically creates a Windows service, as follows:

- Creates a folder named *view n* and a new Windows service named CA Service View n . For both the folder name and service name, the number n is copied from the `view.node.id= $number$` parameter in the `cluster.properties` file.

For example, when you first run this command, suppose you specify `view.node.id=1` in the `cluster.properties` file. In that case, the command creates a folder named `view1` and a new Windows service named CA Service View1.

Similarly, when you run this command for the second time, suppose you specify `view.node.id=2` in the `cluster.properties` file. In that case, the command creates a folder named `view2` and a new Windows service named CA Service View2.

Likewise, when you update the file again and run this command again each successive time, it creates the folder and service, and names them accordingly.

- Runs the following command in `%USM_HOME%\View\bin`:

```
viewservice.bat -i
```

The new Windows Service named CA Service View $number$ is created, where $number$ is the same as the `view.node.id= $number$` parameter in the `cluster.properties` file.

A sample service name is CA Service View3.

- Opens the `viewservice.bat` file and specifies the path name to the `viewservice.conf` for the new service.
- Starts the new service.

This action creates a log file named `tomcat_view $number$.log` in the folder named `%USM_HOME%\logs\view_logs`. The $number$ is the same as the `view.node.id= $number$` parameter in the `cluster.properties` file. A sample file name is `tomcat_view3.log`.

Note: To remove the CA Service View n service, enter the command: `viewservice.bat -r`.

Verify the Server.xml Files

Verifying the `server.xml` files is a required task when you [set up a cluster](#) (see page 220).

To verify the `server.xml` files

1. Review the [updates made by the ant command](#) (see page 222), especially the [updates to the `server.xml` file](#) (see page 222).
2. Open each `server.xml` file and perform the remaining steps.

3. Locate the following line and verify that the file specifies a unique jvm route name:

```
<Engine name="Standalone" defaultHost="localhost" debug="0"  
jvmRoute="_hostname_{usmviewnumber|cawfnnumber}">
```

4. Update the jvm route name to a unique value, if any other server.xml file specifies the same value.

5. Locate the following lines and verify that the file specifies a unique tcplisten port number:

```
<Receiver  
    className="org.apache.catalina.cluster.tcp.ReplicationListener"  
    tcpListenAddress="auto"  
    tcpListenPort="4002"  
    tcpSelectorTimeout="100"  
    tcpThreadCount="6"/> <Receiver
```

6. Update the tcplisten port number to a unique value, if any other server.xml file specifies the same value.

You have verified the server.xml files.

Remove a Cluster

When necessary, you can remove a vertical Service View cluster. Sample reasons for doing so include the following conditions:

- This computer becomes obsolete.
- You want to install clustering on a different computer instead of this one.
- This cluster is no longer needed.

Note: You perform this procedure once for *each* cluster that you want to remove. Each time you perform this procedure, you update the *same* cluster.properties file before you run the ant command.

To remove a cluster

1. Open the cluster.properties file for editing.
2. Specify the number of the cluster to remove in the following parameter, as follows:

view.node.id=number

Specifies the number of the cluster to remove.

For example, to remove Cluster 2, specify the following:

```
view.node.id=2
```

3. Save and close the file.

4. Navigate to %USM_HOME% in Windows Explorer and double-click the usm.cmd file.

The CA Service Catalog command prompt opens, with the location set to the %USM_HOME% folder path.

5. Enter the following command at that prompt:

```
ant uninstall-view-node
```

The cluster specified in the cluster.properties file is removed. The Windows service for that cluster is also removed.

You have removed a cluster node. Next, verify that the [load balancer setup](#) (see page 236) no longer references this cluster.

Set Up Horizontal Clustering for Service View

This process is required to set up horizontal clustering for Service View.

Important! Perform this process on *every* computer on which you want to set up a horizontal cluster node for Service View, including the first Service View computer.

Note: Before you perform this procedure, verify that Service View is installed locally.

To set up horizontal clustering for Service View

1. As a prerequisite, if this computer is not the first-installed Service View computer, do the following:
 - a. Verify that its host name is unique.
 - b. Verify that its database is pointing to the database of the Service View component installed first.
2. Open the %USM_HOME%\view\conf\server.xml file for editing and uncomment the Cluster tags shown in the following lines, if they are commented:

```
<Cluster className="org.apache.catalina.cluster.tcp.SimpleTcpCluster"
  managerClassName="org.apache.catalina.cluster.session.DeltaManager"
  expireSessionsOnShutdown="false"
  useDirtyFlag="true" notifyListenersOnReplication="true">
  <Membership className="org.apache.catalina.cluster.mcast.McastService"
  mcastAddr="228.0.0.4" mcastPort="45564"
  mcastFrequency="500" mcastDropTime="3000" />
  <Receiver className="org.apache.catalina.cluster.tcp.ReplicationListener"
  tcpListenAddress="auto"
  tcpListenPort="4001" tcpSelectorTimeout="100" tcpThreadCount="6" />
  <Sender className="org.apache.catalina.cluster.tcp.ReplicationTransmitter"
  replicationMode="pooled"
  ackTimeout="15000" />
  <Valve className="org.apache.catalina.cluster.tcp.ReplicationValve"
  filter=".*\.(gif|\.js|\.jpg|\.png|\.css|\.txt)" />
  <Deployer className="org.apache.catalina.cluster.deploy.FarmWarDeployer"
  tempDir="/tmp/war-temp"
  deployDir="/tmp/war-deploy/" watchDir="/tmp/war-listen/" watchEnabled="false" />
  <ClusterListener className="org.apache.catalina.cluster.session.ClusterSessionListener" />
</Cluster >
```

- Specify a unique `tcpListenPort` in the `<Cluster>` section. You can find the `tcpListenPort` in the cluster tag of the following line:

```
<Receiver className="org.apache.catalina.cluster.tcp.ReplicationListener" tcpListenAddress="auto"
tcpListenPort="4001" tcpSelectorTimeout="100" tcpThreadCount="6" />
```

For example, suppose the `tcpListenPort` on the first Service View computer is 4001, as shown in the previous line. In that case, the `tcpListenPort` could be 4002 on the second Service View computer, 4003 on the third Service View computer, and so forth. In this way, the `tcpListenPort` is unique on each computer.

- Uncomment the Apache JServ Protocol (AJP) tags shown in the following lines, if they are commented:

```
<Connector port="8009" maxThreads="150" tomcatAuthentication="false" minSpareThreads="25"
maxSpareThreads="75" enableLookups="false" redirectPort="8443" protocol="AJP/1.3" />
```

- Comment the HTTP ports Connector tags. These tags appear similar to the following:

```
<Connector port="8080" enableLookups="true" redirectPort="8443" tomcatAuthentication="false"
acceptCount="100" maxThreads="150" minSpareThreads="25" maxSpareThreads="75" debug="0"
connectionTimeout="20000"
disableUploadTimeout="true" compression="on" compressionMinSize="2048"
compressableMimeType="text/html,text/xml,text/css,text/javascript,image/png,image/gif"
useBodyEncodingForURI="false" URIEncoding="UTF-8" />
```

This step is a best practice and helps improve increased security.

- Save the file.
- Restart the CA Service View service.
- If you are using NTLM authentication to enable single sign-on to CA Service Catalog, [set up NTLM authentication for each cluster](#) (see page 230); otherwise, skip this step.

You have set up horizontal clustering for Service View. After performing this procedure for all Service View clusters, [set up load balancing](#) (see page 236).

Remove a Cluster

When necessary, you can remove a horizontal Service View cluster. Sample reasons for doing so include the following conditions:

- This computer becomes obsolete.
- You want to install clustering on a different computer instead of this one.
- This cluster is no longer needed.

To remove a cluster

1. Open the server.xml file of the horizontal cluster node that you want to remove.
2. Comment the cluster tag
3. Restart the CA Service View service.

You have removed the cluster node. Next, verify that the [load balancer setup](#) (see page 236) no longer references this cluster.

Also, you can optionally [uninstall](#) (see page 331) Service View from the computer whose cluster you removed.

Set Up NTLM Authentication for Each Cluster

If you are using NTLM authentication to enable single sign-on to CA Service Catalog, then setting up each Service View cluster for single sign-on is a required task. This task is required to set up both [vertical clustering](#) (see page 218) and [horizontal clustering](#) (see page 228) for Service View.

Important! This topic applies and is required *only* if you are using NTLM authentication to enable single sign-on in a clustered environment. Otherwise, skip this topic.

Follow these steps:

1. Do *one* of the following:
 - If you are using Apache Load Balancer, [configure NTLM authentication with Apache Load Balancer](#) (see page 231).
 - If you *are* using a load balancer *other than* Apache Load Balancer, [configure NTLM authentication with your load balancer](#) (see page 232).

You have set up NTLM authentication for the clusters.

Configure NTLM Authentication with Apache Load Balancer

Perform the following process to set up NTLM authentication for each cluster, using Apache Load Balancer. If you *are* using Apache Load Balancer, configuring NTLM with Apache Load Balancer is a required task.

Important! This topic applies only if you *are* using Apache Load Balancer!

Follow these steps:

1. Download the mod_auth_sspi module from the sourceforge web site, sourceforge.net.
2. Copy the mod_auth_sspi.so module to the <APACHE_Home>\modules directory of the Apache web server that you use for CA Service Catalog.
3. Append the following configuration section to the <APACHE_Home>\conf\httpd.conf file:

```
LoadModule sspi_auth_module modules/mod_auth_sspi.so
<Location ~ "/usm/(wpf|documents|FileStore)">
AuthName "domain_name"
AuthType SSPI
SSPIAuth On
SSPIOfferBasic On
SSPIAuthoritative On
SSPIDomain "domain_name"
SSPIOfferSSPI off
require valid-user
</Location>
```

4. Update this section: Replace *domain_name* with the name of your network domain or Windows domain.
5. Verify that the tomcatAuthentication="false" attribute is set for the Tomcat connectors that this Apache load balancer uses.

This setting is the default in all server.xml connectors.

6. Log in to CA Service Catalog.
7. Click Administration, Configuration, Single Sign On Authentication.
The Single Sign On Authentication page appears.

8. Do the following:
 - a. Locate the property named Single Sign On Type and click its Modify icon (by default, a pencil).

The Edit Configuration dialog for this property appears.
 - b. Select the option named Artifact Based Single Sign On and click Update Configuration.

Note: In this dialog, you select Artifact Based Single Sign On (not the NTLM option), because you are setting up a cluster.

The dialog closes, and you return to the Sign On Authentication page.
 - c. Locate the property named Artifact Type and click its Modify icon (by default, a pencil).

The Edit Configuration dialog for this property appears.
 - d. Select the option named Request and click Update Configuration.

The dialog closes, and you return to the Sign On Authentication page.

You have configured NTLM authentication to work with Apache Load Balancer.

Configure NTLM Authentication with Another Type of Load Balancer

Perform this procedure to set up NTLM authentication for each cluster, using a load balancer *other than* Apache Load Balancer.

Important! This topic applies only if you are *not* using Apache Load Balancer!

Follow these steps:

1. Set up NTLM authentication, if you want to use NTLM authentication for your load balancer.

Note: For details, see your load balancer documentation.
2. Configure Tomcat to use NTLM authentication for CA Service Catalog for each catalog cluster node, if *both* of the following conditions exist:
 - Your load balancer is not configured to perform NTLM authentication.
 - Your load balancer uses the HTTP Port (default 8080) to connect to Tomcat instances of CA Service Catalog.
3. Log in to CA Service Catalog.
4. Click Administration, Configuration, Single Sign On Authentication.

The Single Sign On Authentication page appears.

5. Do the following:
 - a. Locate the property named Single Sign On Type and click its Modify icon (by default, a pencil).

The Edit Configuration dialog for this property appears.
 - b. Select the option named Artifact Based Single Sign On and click Update Configuration.

Note: In this dialog, you select Artifact Based Single Sign On (not the NTLM option), because you are setting up a cluster.

The dialog closes, and you return to the Sign On Authentication page.
 - c. Locate the property named Artifact Type and click its Modify icon (by default, a pencil).

The Edit Configuration dialog for this property appears.
 - d. Set Artifact Type to the appropriate for your load balancer, for example, Request. Click Update Configuration.

The dialog closes, and you return to the Sign On Authentication page.

You have configured NTLM authentication for a load balancer other than Apache Load Balancer.

Set Up Horizontal Clustering for CA Workflow

This procedure is required to set up horizontal clustering for CA Workflow. Perform this procedure on *every* computer on which you want to set up a horizontal cluster node for CA Workflow, including the first CA Workflow computer.

Note: Before you perform this procedure, verify that CA Workflow is installed locally.

To set up horizontal clustering for CA Workflow

1. As a prerequisite, if this computer is not the first-installed CA Workflow computer, do the following:
 - a. Verify that its host name is unique.
 - b. Verify that its database is pointing to the database of the CA Workflow component installed first.

2. Open the fulfillment\conf\server.xml file on the computer with the original CA Workflow installation. Update the file as follows, and save the file after each update:

- a. Uncomment the Cluster tags shown in the following lines, if they are commented:

```
<Cluster className="org.apache.catalina.cluster.tcp.SimpleTcpCluster"
  managerClassName="org.apache.catalina.cluster.session.DeltaManager"
  expireSessionsOnShutdown="false"
  useDirtyFlag="true" notifyListenersOnReplication="true">
  <Membership className="org.apache.catalina.cluster.mcast.McastService"
    mcastAddr="228.0.0.4" mcastPort="45564"
    mcastFrequency="500" mcastDropTime="3000" />
  <Receiver className="org.apache.catalina.cluster.tcp.ReplicationListener"
    tcpListenAddress="auto"
    tcpListenPort="4001" tcpSelectorTimeout="100" tcpThreadCount="6" />
  <Sender className="org.apache.catalina.cluster.tcp.ReplicationTransmitter"
    replicationMode="pooled"
    ackTimeout="15000" />
  <Valve className="org.apache.catalina.cluster.tcp.ReplicationValve"
    filter=".*\gif;.*\js;.*\jpg;.*\png;.*\css;.*\txt;" />
  <Deployer className="org.apache.catalina.cluster.deploy.FarmWarDeployer"
    tempDir="/tmp/war-temp"
    deployDir="/tmp/war-deploy/" watchDir="/tmp/war-listen/" watchEnabled="false" />
  <ClusterListener className="org.apache.catalina.cluster.session.ClusterSessionListener" />
</Cluster >
```

- b. Specify a unique tcplistenport in the <Cluster> section for each horizontal cluster node that you create on additional CA Workflow computers. You can find the tcplistenport in the cluster tag of the following line:

```
<Receiver className="org.apache.catalina.cluster.tcp.ReplicationListener" tcpListenAddress="auto"
  tcpListenPort="4001" tcpSelectorTimeout="100" tcpThreadCount="6" />
```

For example, suppose the tcpListenPort on the first CA Workflow computer is 4001, as shown in the previous line. In that case, the tcpListenPort could be 4002 on the second CA Workflow computer, 4003 on the third CA Workflow computer, and so forth. In this way, the tcpListenPort is unique on each computer.

- c. Uncomment the Apache JServ Protocol (AJP) tags shown in the following lines, if they are commented:

```
<Connector port="8019" enableLookups="false" redirectPort="8443" protocol="AJP/1.3"
emptySessionPath="true" />
```

- d. Comment the HTTP ports Connector tags, as follows:

```
<!--<Connector port="8090" minProcessors="5" maxProcessors="200"
enableLookups="true" redirectPort="8443"/>-->
```

This action is a best practice and helps increase security.

3. Save and close each file.
4. Restart the CA Workflow service. It is named CA Service Fulfillment.

You have set up horizontal clustering for CA Workflow. You are now ready to [set up load balancing](#) (see page 236).

Remove a Cluster

When necessary, you can remove a [horizontal cluster for CA Workflow](#) (see page 233). Sample reasons for doing so include the following conditions:

- This computer becomes obsolete.
- You want to install clustering on a different computer instead of this one.
- This cluster is no longer needed.

To remove a cluster

1. Open the server.xml file of the horizontal cluster node to be removed.
2. Comment the cluster tag
3. Restart the CA Service Fulfillment service.

You have removed the cluster node. Next, verify that the [load balancer setup](#) (see page 236) no longer references this cluster.

Also, you can optionally [uninstall](#) (see page 331) CA Workflow from the computer whose cluster you removed.

How to Set Up Load Balancing

To load balance the existing nodes using Apache HTTP Server, follow these instructions. This process applies to all types of Service View and CA Workflow clusters. Perform this process *after* you have set up all cluster nodes.

1. Install Apache HTTP Server 2.2.16. It is included with the CA Service Catalog installation media.

Note: For instructions, see the Apache HTTP Server documentation.

The default installation folder is C:\Program Files\Apache Software Foundation\Apache2.2.

2. [Configure Apache HTTP Server](#) (see page 236).
3. (Optional) [Disable web server features](#) (see page 237).
4. [Create and configure the workers.properties file](#) (see page 238).
5. [Create the uriworkermap.properties file](#) (see page 246).
6. [Update the httpd.conf file](#) (see page 247).
7. [Disable the HTTP Ports of the cluster computers](#) (see page 249).
8. [Verify load balancing](#) (see page 250).

Configure Apache HTTP Server

Configuring Apache HTTP Server is a required task when you [set up load balancing](#) (see page 236).

To configure Apache HTTP Server

1. Access the Apache website, www.apache.org.
2. Find and download the file named `mod_jk-1.2.30-httpd-2.2.3.so`. At publication time, this file is available in Apache Tomcat Connector section of the website.
CA Service Catalog supports `mod_jk 1.2.30`.
3. Rename the `mod_jk-1.2.30-httpd-2.2.3.so` file to `mod_jk.so`.
4. Copy the `mod_jk.so` file to the modules folder in the Apache Server installation.

You have configured Apache HTTP Server.

Disable Web Server Features

Disabling the web server features of Apache HTTP Server is an *optional* task when you [set up load balancing](#) (see page 236). Because Apache HTTP Server is used as a load balancer, you can *optionally* perform these cleaning steps to disable the Apache *web server* features. Doing so improves performance and reduces potential security risks. If you use this version of Apache HTTP Server for other services or if you have other reasons, you can skip this procedure.

To disable web server features

1. Delete the following folders under C:\Program Files\Apache Software Foundation\Apache2.2:

Note: In this step and other steps in this process, the "C:\Program Files\" portion of the path names reflect the typical location specified at installation time. This portion of your path names can vary, depending, for example, on the installation directory specified for the \Apache Software Foundation folder at installation time.

- \cgi-bin
 - \error
 - \htdocs
 - \icons
 - \manual
2. Rename httpd.conf to _httpd.conf.bak in the C:\Program Files\Apache Software Foundation\Apache2.2\conf directory.
 3. Find the httpd.minimal.conf file.

This minimal configuration file is included in the Utilities/Apache Webserver directory of the CA Service Catalog installation media.
 4. Copy the httpd.minimal.conf file to C:\Program Files\Apache Software Foundation\Apache2.2\conf.
 5. Rename the httpd.minimal.conf file to httpd.conf in that directory.
 6. Delete all files in that directory *except* the following:
 - httpd.conf
 - _httpd.conf.bak

7. Change to the C:\Program Files\Apache Software Foundation\Apache2.2\modules directory.
8. Delete all files in that directory *except* the following:
 - mod_jk.so
 - mod_log_config.so
 - mod_setenvif.so

You have disabled web server features.

How to Create and Configure the workers.properties File

Creating and configuring the worker.properties file is a required task when you [set up load balancing](#) (see page 236). To create and configure the worker.properties file, follow this process:

1. Create the workers.properties file manually in the \conf directory of the Apache installation folder.
2. Verify that the file lists all the Tomcat instances to include in the clustered environment.
3. Obtain the following information for each cluster node:

- The host name of the clustered node
- The ajp port of the clustered node. Obtain it from the connector port in the following line in the server.xml file of each cluster node:

```
<Connector port="8009" maxThreads="150" tomcatAuthentication="false" minSpareThreads="25" maxSpareThreads="75" enableLookups="false" redirectPort="8443" protocol="AJP/1.3" />
```

- The jvmRoute name of the node; obtain it from the following line in the server.xml file of each cluster node:

```
<Engine name="Standalone" defaultHost="localhost" debug="0" jvmRoute="hostname_usmview">
```

For example, for the Service View cluster node on the computer named XYZ, the jvmRoute name is XYZ_usmview.

Important! Verify that the jvmRoute name is unique for each Service View and CA Workflow cluster. This name must be unique, because the load balancer uses it to identify each cluster. This name is case-sensitive!

4. Review the following sample worker.properties file sections for the types of clustering that you can perform with Service View and CA Workflow.

In all cases, the worker.properties file defines a load balancer node named loadbalancerview. This node balances Service View requests among the Service View cluster nodes. For example, this node load balances the /usm context between the workers defined. The context path /usm is defined in the %USM_HOME%\view\conf\server.xml file pointing to the Service View web application.

The examples illustrate each type of clustering:

- [Horizontal clustering example for Service View](#) (see page 241)
- [Vertical clustering example for Service View](#) (see page 242)
- [Horizontal clustering example for CA Workflow](#) (see page 243)
- [Horizontal clustering example for both Service View and CA Workflow](#) (see page 245)

5. Add a new worker to the cluster, as follows:

- a. Create a worker section at the end of the worker.properties file, using the following lines as a model:

```
worker.jvmRouteName.port=ajpport
worker.vmRouteName.host=HOSTNAME
worker.jvmRouteName.type=ajp13
worker.jvmRouteName.lbfactor=1
```

- b. Verify that its jvmRouteName is unique.
- c. Add the new cluster at the end of the list of balance workers for a loadbalancer node.

For example, suppose the jvmRoute name of the new worker is COMPUTER3_cawf and its ajpport is 8019. In that case, enter the following new worker section to add the new cluster to the selected loadbalancer node:

```
worker.COMPUTER3_cawf.port=8019
worker.COMPUTER3_cawf.host= COMPUTER3
worker.COMPUTER3_cawf.type=ajp13
worker.COMPUTER3_cawf.lbfactor=1
```

6. Remove an existing cluster from the loadbalancer setup in the worker.properties file, as follows:
 - a. Delete the section for the worker.
 - b. Remove any references to the deleted worker from the list of balance workers.
The list of balance workers begins with the following line:
`worker.<loadbalancemode>.balance_workers`
7. [Update the URL for horizontal clustering of CA Workflow](#) (see page 245).

You have created and configured the worker.properties file.

Horizontal Clustering Example for Service View

This example illustrates how to use horizontal clustering to load balance the /usm context of Service View between two workers (clusters) whose specifications are as follows:

Worker1:

- Hostname: Computer1
- JVMroutename: Computer1_usmview
- AJP port: 8009

Worker 2:

- Hostname: Computer2
- JVMroutename: Computer2_usmview
- AJP port: 8009

In these examples, Computer1 and Computer2 are the host names (computer names) of the workers.

You can use the loadbalancerview node to load balance between the workers Computer1 and Computer2 as horizontal clusters for Service View. To do so, define the loadbalancerview node sections of the worker.properties as follows. Use these sections as a model to configure your workers.properties file.

```
worker.list=loadbalancerview
```

```
worker.status.type=status
```

```
worker.loadbalancerview.method=Busyness
```

```
worker.loadbalancerview.type=lb
```

```
worker.loadbalancerview.balance_workers=COMPUTER1_usmview,COMPUTER2_usmview
```

```
worker.loadbalancerview.sticky_session=1
```

```
worker.COMPUTER1_usmview.port=8009
```

```
worker.COMPUTER1_usmview.host=COMPUTER1
```

```
worker.COMPUTER1_usmview.type=ajp13
```

```
worker.COMPUTER1_usmview.lbfactor=10
```

```
worker.COMPUTER2_usmview.port=8009
```

```
worker.COMPUTER2_usmview.host=COMPUTER2
```

```
worker.COMPUTER2_usmview.type=ajp13
```

```
worker.COMPUTER2_usmview.lbfactor=10
```

Vertical Clustering Example for Service View

This example illustrates how to use vertical clustering to load balance the /usm context of Service View between two workers (clusters) whose specifications are as follows:

Worker 1:

- Hostname:COMPUTER1
- JVMroutename:COMPUTER1_usmview
- AJP port :8009

Worker 2:

- Hostname:COMPUTER1
- JVMroutename:COMPUTER1_usmview1
- AJP port :8010

Sample sections follow of the workers.properties file that use these settings. Use these sections as a model to configure your workers.properties file.

```
worker.list=loadbalancerview  
worker.status.type=status
```

```
worker.loadbalancerview.method=Busyness  
worker.loadbalancerview.type=lb  
worker.loadbalancerview.balance_workers=COMPUTER1_usmview,COMPUTER2_usmview1  
worker.loadbalancerview.sticky_session=1
```

```
worker.COMPUTER1_usmview.port=8009  
worker.COMPUTER1_usmview.host=COMPUTER1  
worker.COMPUTER1_usmview.type=ajp13  
worker.COMPUTER1_usmview.lbfactor=10  
worker.COMPUTER1_usmview1.port=8010  
worker.COMPUTER1_usmview1.host=COMPUTER2  
worker.COMPUTER1_usmview1.type=ajp13  
worker.COMPUTER1_usmview1.lbfactor=10
```

Horizontal Clustering Example for CA Workflow

The `worker.properties` file uses the `loadbalancerwf` node to load balance CA Workflow requests between the CA workflow cluster nodes. For CA Workflow, the `loadbalancerwf` node load balances the `/wl`, `/pm`, and `/usm_idews` contexts between the defined workers. A description of each context follows:

- `/wl` is specified in the `%USM_HOME%\fulfillment\conf\Catalina\localhost\wl.xml` file; it points to the `wl(worklist)` web application of CA Workflow
- `/pm` is specified in the `%USM_HOME%\fulfillment\conf\Catalina\localhost\pm.xml`; it points to the process manager (`pm`) web application of CA Workflow
- `/usm_idews` is the IDE application of CA Workflow

These contexts are already defined in the files mentioned. However, to cluster these contexts, [update the `httpd.conf` file](#) (see page 247) with them.

This example illustrates how to use horizontal clustering to load balance CA Workflow requests between two workers (clusters) whose specifications are as follows:

Worker1:

- `Hostname:COMPUTER1`
- `JVMroutename:COMPUTER1_cawf`
- `AJP port :8019`

Worker 2:

- `Hostname:COMPUTER2`
- `JVMroutename:COMPUTER2_cawf`
- `AJP port :8019`

Sample sections of the `workers.properties` file that use these settings appear as follows. Use these sections as models to configure your `workers.properties` file.

```
worker.list=loadbalancervf
worker.status.type=status

worker.loadbalancervf.method=Busyness
worker.loadbalancervf.type=lb
worker.loadbalancervf.balance_workers=COMPUTER1_cawf,COMPUTER2_cawf
worker.loadbalancervf.sticky_session=1

worker.COMPUTER1_cawf.port=8019
worker.COMPUTER1_cawf.host=COMPUTER1
worker.COMPUTER1_cawf.type=ajp13
worker.COMPUTER1_cawf.lbfactor=10
worker.COMPUTER2_cawf.port=8019
worker.COMPUTER2_cawf.host=COMPUTER2
worker.COMPUTER2_cawf.type=ajp13
worker.COMPUTER2_cawf.lbfactor=10
```

Note: Vertical clusters do *not* apply to CA Workflow.

Horizontal Clustering Example for Both Service View and CA Workflow

An example of a horizontal cluster for both Service View and CA Workflow follows. You can optionally use it and the other examples to edit the `worker.properties` file to set up your own horizontal cluster for *both* Service View and CA Workflow.

```
worker.list=loadbalancerwf, loadbalancerview
worker.status.type=status

worker.loadbalancerwf.method=Busyness
worker.loadbalancerwf.type=lb
worker.loadbalancerwf.balance_workers=COMPUTER1_cawf,COMPUTER2_cawf
worker.loadbalancerwf.sticky_session=1
worker.loadbalancerview.method=Busyness
worker.loadbalancerview.type=lb
worker.loadbalancerview.balance_workers=COMPUTER1_usmview,COMPUTER2_usmview
worker.loadbalancerview.sticky_session=1
worker.COMPUTER1_cawf.port=8019
worker.COMPUTER1_cawf.host=COMPUTER1
worker.COMPUTER1_cawf.type=ajp13
worker.COMPUTER1_cawf.lbfactor=10
worker.COMPUTER2_cawf.port=8019
worker.COMPUTER2_cawf.host=COMPUTER2
worker.COMPUTER2_cawf.type=ajp13
worker.COMPUTER2_cawf.lbfactor=10
worker.COMPUTER1_usmview.port=8009
worker.COMPUTER1_usmview.host=COMPUTER1
worker.COMPUTER1_usmview.type=ajp13
worker.COMPUTER1_usmview.lbfactor=10
worker.COMPUTER2_usmview.port=8009
worker.COMPUTER2_usmview.host=COMPUTER2
worker.COMPUTER2_usmview.type=ajp13
worker.COMPUTER2_usmview.lbfactor=10
```

Update the URL for Horizontal Clustering of CA Workflow

If you are implementing horizontal clustering for CA Workflow, update the URL in the `pm.xml` and `wl.xml` files to point to the load balancer port. This task is required to set up the cluster successfully.

To update the URL for horizontal clustering for CA Workflow

1. Shut down the Windows service for CA Workflow, which is named CA Fulfillment.
2. Open the `pm.xml` file for editing. This file is located in the `%USM_HOME%\fulfillment\conf\Catalina\localhost` folder.

3. Locate the following line and update it to be as follows; this line is named the defaultpmurl:

```
http://<load balancer>:<port-number>/pm/
```

load balancer

Specifies the name of the load balancer computer for CA Workflow.

port-number

Specifies the port number on that computer used to listen for incoming requests for CA Workflow.

4. Save the pm.xml file.
5. Repeat steps 2-4 for the wl.xml file.
6. Delete the %USM_HOME%\fulfillment\work\Catalina directory.
7. Restart the Windows service named CA Fulfillment.
8. Repeat these steps for each cluster.

You have updated the URL for horizontal clustering of CA Workflow.

Create the uriworkermap.properties File

Creating and configuring the uriworkermap.properties file is a required task when you [set up load balancing](#) (see page 236). This file specifies which context the load balancer node selects and forwards to its cluster nodes.

Note: If the file exists already, update it to match the text in the following steps.

To create the uriworkermap.properties file

1. Manually create the uriworkermap.properties file in the \conf directory of the Apache installation folder.
2. Enter the following lines in the file:

```
/usm/*=loadbalancerview  
/pm/*=loadbalancerwf  
/wl/*=loadbalancerwf  
/usm_idews/*=loadbalancerwf
```

Note: The first line is for Service View clustering. The remaining lines are for CA Workflow clustering.

3. Save the file.

You have created the uriworkermap.properties file.

Update the httpd.conf File

Updating the httpd.conf file is a required task when you [set up load balancing](#) (see page 236).

To update the httpd.conf file

1. Open the conf/httpd.conf file in the Apache HTTP Server installation directory and update it to include the following specifications:

```
Listen 89
LoadModule jk_module modules/mod_jk.so
JkWorkersFile conf/workers.properties

<VirtualHost *:89>
    ServerName load balancer host name

    JkMountFile conf/uriworkemap.properties
    JkLogFile logs/mod_jk.log
    JkLogLevel debug
</VirtualHost>
```

2. Find the following lines:

```
JkLogFile logs/mod_jk.log
JkLogLevel debug
```

3. (Optional) Replace the lines in the previous step with the following lines:

```
JkLogFile "|bin/rotatlogs.exe logs/mod_jk.log.%Y-%m-%d-%H_%M_%S 10M"
JkLogLevel emerg
```

This action modifies the mod_jk.log file on your production server to record only critical errors and to enable log automatic rollover when its file size reaches 10 MB.

4. Add a Listen directive with the port number for every VirtualHost port in the file.

For example, suppose you have defined a virtual host at port 89, as follows:

```
<VirtualHost *:89>
```

In that case, add the Listen directive for this port in the httpd.conf file, for example:

```
Listen 89
```

Note: The commonly used port is 89.

This specification enables the Apache HTTP Server to listen on this port and accept incoming requests.

5. Change the Default Type from text/plain to text/html.

Note: This setting works well on most browsers. If you experience any difficulty with system performance or display quality after changing this option, return it to its original value.

6. Save and close the conf/httpd.conf file.
7. [Adjust related settings](#) (see page 248) in other locations.

8. [Disable the HTTP ports of the cluster computers](#) (see page 249).

You have updated the `httpd.conf` file.

Adjust Related Settings

Adjusting related settings is a required task when you [update the `httpd.conf` file](#) (see page 247).

To adjust related settings

1. Open your web browser and set the proper values for the `ServerAdmin` and `ServerName` options, if you have not done so.
2. Restart the Apache service, as follows:
 - a. Open the Apache Service Monitor.
 - b. Highlight the service to restart.
 - c. Click Restart.
3. Test by accessing the link `http://loadbalancerhostname:89/wl` or any other context for CA Workflow and `http://hostname:89/usm` for Service View.

Here, *hostname* specifies the load balancer computer, that is, the computer on which the Apache HTTP Server is configured for load balancing. For example, if the host name of the load balancer computer is ABC, then the link is `http://ABC:89/wl`.

4. Review the `mod_jk.log` file under the `logs` folder in the Apache directory to determine which `jvmRoute` node was called. An example follows:

```
found worker HOST1__USMView (HOST1__USMView) for route COMPUTER1__USMView and partial  
sessionId
```

You have adjusted settings related to the `httpd.conf` file.

Disable the HTTP Ports of the Cluster Computers

Disabling the HTTP ports of the cluster computers is a required task when you [update the httpd.conf file](#) (see page 247). Doing so routes users directly to the load balancer computer rather than directly to a cluster.

To disable the HTTP ports of the cluster computers

1. Do the following in the server.xml files of each cluster computer: Comment the connector tag that includes HTTP port information. This port is the startup node provided during installation, typically 8080 for Service View and 8090 for CA Workflow.
 2. Do the following on the CA Service Catalog GUI:
 - a. Click Administration, Configuration, Server Information.
The server configuration options appear.
 - b. Replace the server host name and port number with the load balancer host name and port number.
These options are updated.
 3. Recycle Windows services of the clusters whose server.xml files were changed.
 4. Do the following on the CA Service Catalog GUI:
 - a. Click Administration, Configuration, Workflow.
The CA Workflow configuration options appear.
 - b. Replace the CA Workflow host name and port number with the load balancer host name and port number.
These options are updated.
- Note:** If you have not clustered CA Workflow or if you are not using CA Workflow, skip this step and go to the next step.
5. Click the Configure button.
The CA Workflow actors are updated with the new URLs.
 6. Recycle the Windows services of the clusters whose server.xml files were changed.

You have disabled the HTTP ports of the cluster computers.

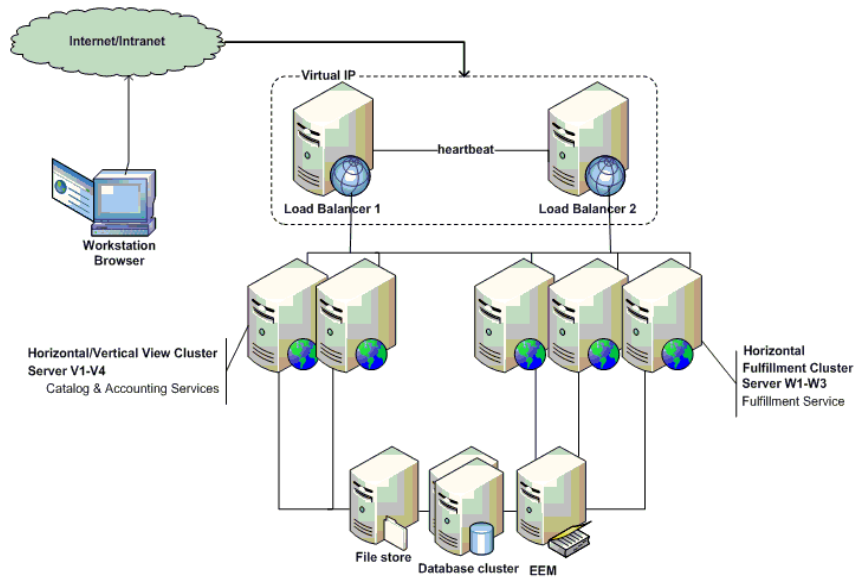
How to Verify Load Balancing

Verify your load balancing setup to help ensure that it runs efficiently. To verify your load balancing setup, follow this process:

1. Sanity test the implementation, as follows:
 - To test failover functionality, verify that the load is distributed to other nodes when one of the nodes in the same cluster shuts down.
 - To test load balancing, verify that the load is distributed to other nodes when one of the nodes in the same cluster becomes busy.
2. If you add or delete clusters after your initial setup, use the previous steps as a model to do the following: Update the `workers.properties` files to add the new cluster or remove the deleted cluster.
3. We recommend that you cluster your load balancer computers to help avoid single-point-of-failure problems with an individual load balancer computer. For instructions, see the Apache website, www.apache.org, and other resources with expertise in clustering load balancer computers.
4. Verify that *all* clustered nodes for Service View and CA Workflow communicate efficiently with *all* load balancer computers using the telnet utility.
5. If clusters do not run efficiently, verify that this communication exists and check for any network configuration problems. For example, in the following diagram, all the computers V1-V4 and W1-W3 clusters must be able to run the “telnet loadbalancer portno” command.

For example, suppose your load balancer host name is `abc` and the port is `89`. In that case, verify that you can successfully connect from all your clustered nodes. To do so, enter the following command from each node:

```
telnet abc 89
```



Chapter 11: Best Practices

This section contains the following topics:

[Overview](#) (see page 253)

[Benefits](#) (see page 254)

[Guidelines for Collecting Data](#) (see page 255)

[Best Practices Foundation](#) (see page 258)

[Guidelines for Customizing Catalog Content](#) (see page 263)

Overview

Historically, IT organizations have focused on technology without clear accountability for adding business value, while their customers have focused on costs. Increased competition in the marketplace and increased dependence on high technology demand that IT organizations do the following:

- Build a stronger understanding of the customers they serve
- Work in a close partnership with them to deliver true value

These business alignment initiatives require the following:

- A clear definition of the services that the IT organization provides
- An understanding of the components and resources that constitute the services
- An identification of the costs of the associated services

With centralization of IT services and movement toward a utility model, implementing a service catalog becomes an increasingly important necessity. Using a service catalog leads to better IT service alignment with business goals and improved internal customer satisfaction. It also leads to standardized processes to achieve greater operational efficiency.

The ITIL™ (IT Infrastructure Library) framework stipulates that IT organizations start their process enhancement initiatives by developing a service catalog to do the following:

List all the services being provided

Summarize the details of the services, customers, service designers, and service administrators

Many IT groups produce a service catalog as part of their ITIL Service Level Management deployment. Others view the opportunity to leverage the service catalog as the focal point for communication between IT and the business.

Benefits

CA Service Catalog Best practices offer examples and a starting point for building your own catalog.

CA Service Catalog enables you to load catalog content and to enable related business process automation through using CA Workflow or CA Process Automation. The goal of this initiative is not to create a complete and comprehensive list of services. Instead, the goal is to help you get started in building your own catalog.

As the foundation for aligning IT with the business, the service catalog represents a crucial element of success in ITIL initiatives. By using a service catalog, IT organizations can do the following:

- Create clear service definitions
- Define service levels and costs
- Deliver usage and performance data in business terms
- Track user subscriptions and service requests
- Provide a fast, consistent, and more effective access to IT services
- Publish or review service reports

Developing a service catalog can also provide the following improvements to drive down costs while still achieving high levels of service:

- Improved efficiencies in handling incoming requests
- Eliminate service redundancies
- Increased IT staff productivity
- Better allocation of resources
- Reduced calls to the help desk

Guidelines for Collecting Data

The following guidelines are for using staff interviews to collect data regarding the services and service levels currently existing in your organization. These guidelines are developed based on ITIL Methodology and CobiT™ Principles. These guidelines consist of the following activities for collecting and analyzing data, in sequential order:

- Review of the [purpose of the staff interviews](#) (see page 255)
- Use of the suggested [questions](#) (see page 256) and any related questions of your own to conduct the [staff interviews](#) (see page 256)
- Analysis of service-related [documents](#) (see page 257)
- [Review and benchmark activities](#) (see page 257) for existing services
- Collation the [results of staff interviews](#) (see page 258)
- Organization of the newly determined information into [service specifications](#) (see page 269) that include detailed descriptions of each service

Purpose of the Staff Interviews

The purpose of the interviewing the staff is to obtain and understand organization-wide policies and procedures relating to provider-to-user relationships. Examples follow:

- IT policies and procedures relating to the following:
 - Service level agreements
 - Operational reporting content, timing and distribution
 - Performance tracking methods
 - Corrective action activities
- IT documentation relating to the following:
 - Service level performance reports
 - Service budget and costing procedures
 - Charge-back algorithms and methodology for calculating charges
 - Service improvement programs
 - Recourse resulting from nonperformance
 - Service level agreements with internal and external users and providers of services

Questions for Staff Interviews

The staff interviews can include the following questions:

- Who delivers which services where, to which organization or organizational groups, and at what cost?
- Who requests which services from which IT group and at what volume?
- What level of service is currently in place within the organization?
- Who are the stakeholders?
- How can we use the template catalog?

Staff Interviews

The staff whom you interview include the following:

- Chief Information Officer
- IT senior management
- IT Contract Administrator
- Service Level Administrator
- IT Operations management
- User management

Documents to Analyze

You review and analyze the following documents:

- Service level agreement process
- Definitions of responsibilities of users and providers
- Management reports on the achievement of the specified service performance criteria and all problems encountered

The purpose of analyzing the documents is to verify whether the following conditions exist:

- Users understand service level agreement processes and procedures.
- The level of user satisfaction with the service level process and service level agreements is sufficient.
- Service fulfillment data is available to track performance.
- A performance improvement program exists.
- The accuracy of actual charges matches agreement content.
- A comparison of historical performance and prior service improvement commitments is tracked.
- Managers appropriately use reports on service performance

Review and Benchmark Activities

The review and benchmark activities are as follows:

- Benchmarking of service level agreements against similar organizations or appropriate international standards and recognized industry best practices
- Review of service level agreements to determine qualitative and quantitative provisions confirming obligations are defined and being met
- Review of selected service level agreements to confirm compliance and resolution procedures for problems, specifically nonperformance

Results of Staff Interviews

The results of the staff interviews help the organization identify the following:

- Adequacy of the provisions describing, coordinating, and communicating the relationship between the providers and the users of information services
- Incorrect calculations for selected categories of information
- Ongoing review and corrective action by management of service level reporting
- Adequacy of proposed service improvements in comparison with cost-benefit analysis
- Adequacy of the ability of providers to meet commitments for improvements

Best Practices Foundation

The best practices foundation includes the following:

- [Request and fulfillment automation with CA Workflow and CA Process Automation](#) (see page 258)
- [Service Catalog logical structure](#) (see page 260)
- [Customer-focused documentation](#) (see page 262)

Request and Fulfillment Automation with CA Workflow and CA Process Automation

A key characteristic of the predefined foundation content is the automation of approvals and notifications for actions that complete the service fulfillment process. This automation makes the services "actionable." Service designers accomplish this goal through the workflow capabilities included with CA Workflow and CA Process Automation.

All services in the predefined foundation content invoke the workflow-driven approval process. This process sends an email to the manager of the requestor, indicating the requiring approval for the request. The email includes a link to the approval page in CA Service Catalog to streamline the approval process. To use a different approval process for individual services, select a different approval mechanism for those services through the Service Builder.

After a service request has been approved, the requested items in the service option group then follow a fulfillment workflow. The category specified for the requested component determines the workflow. The predefined service option groups contain components that belong to one of these categories: Hardware, Software, or Service.

The event rules for each category control the notifications generated as the components of the request move through the stages of fulfillment. The foundation content, as delivered, follows the predefined rules for each category. You can customize these rules to address your specific requirements.

The predefined foundation content provides a [category-class-subclass structure](#) (see page 259) for your use.

Category-Class-Subclass Structure

The predefined foundation content provides a category-class-subclass structure. You can use the class and subclass designations within each category to customize the workflow process. The default structure contains the following top-level categories:

- None
- Hardware
- Reservation Manager
- Service
- Service Offering Management
- Software
- Other

Multiple classes exist within each category, and in most cases multiple subclasses within each class.

To view and optionally update the complete detailed structure of category classes and subclasses, [edit the category.xml file](#) (see page 295).

Note: You can add categories to meet your specific requirements. However, you cannot change the internal numeric values of the default categories because this field is used for logic in other portions of the product.

Service Catalog Logical Structure

You can use a table or spreadsheet to design the full logical structure of the catalog before its actual implementation. This approach facilitates communication between stakeholders and end users regarding the service catalog structure and content required.

We recommend that you agree on the general service catalog content and structure first and the details next. As the catalog and its use mature within an organization, some restructuring and fine-tuning are likely to occur.

An example of the logical structure of the catalog, including both the Folder/Service structure and the category-class-subclass specification is illustrated in the following table:

IT Support Services						
Folder	Service	Service Option	Category	Class	Subclass	Description
Data Security						

	Virus Protection / Remediation Plan SLA					
		Bronze	Service	IT	SLA	Bronze SLA for Virus Protection/Remediation
		Silver	Service	IT	SLA	Silver SLA for Virus Protection/Remediation
		Gold	Service	IT	SLA	Gold SLA for Virus Protection/Remediation
	VPN Access					
		Request VPN Access	Service	IT	Security	Request VPN access for remote user
	Proxy Access					
		Subscribe to Proxy	Service	IT	Security	Request proxy access (security request)
	Pre-Production Security Scans					
		Security Scan	Service	IT	Security	Request Security Scan before production status
Data Management						
	Backup Data					
		Backup Production Server Data	Service	IT	Data	Backup Services for Production Server Data
		Backup Local PC / Laptop Data	Service	IT	Data	Backup Services for Local PC / Laptop Data

	Restore Data					Services to restore production or local data
		Restore Production Server Data	Service	IT	Data	Restore data on a production server from backup files
		Restore Local PC / Laptop Data	Service	IT	Data	Restore data on a local PC from backup files

We recommend limiting the number of levels that users navigate to reach specific services in your catalog. As an example, consider an IT Support Services category such as Hardware and Software Procurement. For ease of use, divide it into two separate categories. Examples include Hardware Procurement and Software Procurement. This approach is more efficient than using subfolders, for example, under Hardware and Software Procurement.

You can customize the structure of the provided content to meet the needs of your organization. For example, you can divide a single Server service into the following services: Blade Server, Standard Server, and Mainframe Server. In this case, create a folder named Server to contain the other three services. Each service contains descriptions and service option group items to assist users in their selection.

Customer-Focused Documentation

Prepare customer-focused documentation for the service catalog and make it available to all potential users. Sample contents follow:

- Forward from the IT Director
- Table of Contents
- IT Service Provider profile
- Version number, date created, date amended
- Changes from last published Catalog
- Service times and accessibility of the IT Service Provider
- Overview of Services and Products
- Customer-focused Service and Product descriptions
- Specifications of Services
- Deliverables

- Service Times
- Maintenance Times
- Support Times
- Delivery Times
- Quality Target (availability, reliability, usability, priority)
- Requirements
- Request and Change procedures
- Contingency policy
- Pricing and Charging
- Index and definitions

Guidelines for Customizing Catalog Content

The Best Practice Foundation content on the installation media is a starting point of best practices for setting up your own catalog. When you modify the catalog content, follow these guidelines, mostly in sequential order, but with iteration as needed:

- Install all content onto a test system, and then browse and understand the default catalog content
- Review the [frequently asked questions](#) (see page 264)
- Understand the basic structure of [catalog entries](#) (see page 265)
- Understand the main parts of a [service specification](#) (see page 269), and view the [sample service specification](#) (see page 271) for further details
- Illustrate the fulfillment of the service as steps in a business process that you can follow logically
- Create a detailed logical design in a spreadsheet or flowchart, to help you design the service in the Service Builder
- Determine what parts of the default catalog you want to customize in your production catalog
- On subsequent installations, load only those sections of the content that fit into your test catalog
- Configure all customizations in a test catalog; test and refine them until you approve them
- Copy only the approved modifications into your production catalog
- Consider maintaining a separate development catalog in addition to a test catalog, so that testing and development can occur in parallel

Frequently Asked Questions

The following information provides answers to frequently asked questions and includes instructions for managing your catalog content.

Note: Several questions and answers mention the ixutil utility for importing and exporting catalog entries. For instructions to use the ixutil utility, see the *Reference Guide*.

How do I modify the catalog content?

You modify catalog content by using the standard Service Builder component of the web browser user interface.

Note: For instructions, see the *Administration Guide*.

How do I back up, import, and export catalog content?

Back up any customized content you have created, both before and after customizing. Use the ixutil utility to back up the content, to export it from one system, and to import it into another system.

How do I make bulk changes to the catalog content?

You can make bulk changes to the catalog, as follows:

1. Export the catalog folder or service to be changed, using the IXUTIL utility.
2. Edit the exported XML file using a text editor.
3. Delete and reimport the folder into the catalog.

This process works well for simple changes in descriptions and naming conventions. For example, suppose your IT organization is named General Information Services (GIS). In that case, consider a bulk change to replace the word "IT" with "GIS" within the catalog.

If you are not familiar with using a text editor for editing XML files, obtain assistance from an experienced user. Be especially careful to use a text editor like Notepad, not a word processor like Microsoft Word.

Also follow these guidelines:

- Be careful and back up frequently. If referential integrity issues occur, the import process does not always import all content.
- Review the ixutil.log in the %USM_HOME%\logs\install folder after each import. Review it for duplicate name errors and other errors caused by incorrect syntax in the imported data.

How do I copy catalog entries from test catalogs to production catalogs?

Do the following:

1. Use a test catalog to customize the default catalog content.
2. Back up the test catalog.
3. Export the updated catalog content from the test catalog.
4. Import the updated catalog content into your production catalog.

The two entities included in your catalog are the catalog entries themselves and the images and URL links associated with them.

Use the ixutil utility to export the catalog entries from the test catalog and to import them into the production catalog.

The catalog entries include folders, services, service option groups, and service option elements.

Copy the following to the production environment separately: category, class, and subclass definitions (category.xml), images, and status definitions.

Catalog Entries

As an administrator, you use the Service Builder to create and maintain catalog entries. The following types of catalog entries exist:

- [Folders](#) (see page 266)
- [Services](#) (see page 266)
- [Service option groups](#) (see page 267)
- [Service options](#) (see page 267)
- [Images](#) (see page 269)
- [Category, class, and subclass](#) (see page 269)

Understand these types before you create or modify catalog entries.

Large numbers of entries in a single container can be difficult for catalog users to navigate. Therefore, as a general guideline, we recommend that you limit the number of entries in a container to ten. For example, verify that no folder contains more than ten subfolders or services. Similarly, verify that no service contains more than ten service options, and so on.

Note: The Best Practice Content: Foundation does *not* add new statuses to the predefined statuses in CA Service Catalog.

Folders

The installation process creates the folders that you select. If you select all folders, then the installation process creates the following top-level folders:

- IT Services
- Telecom Services
- Network Services
- Application Services
- Project Services
- Corporate Services
- Personnel Services
- Facilities Services
- Reservation Services

The names of the folders and services in your catalog must be unique.

If you create your own folders, you can name them any unique name. You can create additional content or delete content from the predefined folders. We recommend short descriptive names for folders.

Services

The catalog supports services that contain multiple service option groups. In this starter implementation, however, most services contain one associated service option group. As the catalog designer, you decide to use either one or multiple service option groups per service. In both cases, we recommend that you organize related service option groups in services logically and intuitively.

Focus on the user when designing services and service option groups. A common flaw in catalog design is placing service option groups in a nonintuitive service or folder. When service option groups in a service or folder are unrelated, users have difficulty finding the services they want. For example, consider a service option group for a network design program. You could place it in a service or folder named Development Tools. However, such a service option group fits better in a service or folder named Miscellaneous Software. A network administrator is more likely to view the latter folder first for this program.

The catalog provides a search tool that can be helpful. This tool supplements thoughtful design, but does not replace it.

Service Option Groups

Most service option groups in the predefined catalog are named the same as the corresponding service, for simplicity. They have multiple service options contained within them.

As your catalog becomes more mature, this one-to-one relationship between services and service option groups is likely to decrease. Some examples of having multiple service option groups in a service exist in the "Procure Laptop" and "Procure Desktop" services. The hardware configuration of laptops and desktops have differences. However, the standard and optional software bundled with them is typically identical. Therefore, the catalog does not duplicate the service options related to software choices in the two services. Instead, both services include service option groups for standard and optional software bundles.

Naming conventions become more important as the number of services and service option groups increases. The naming standards are as follows:

- All folders and services have unique names
- If a service contains only one service option group, their names are the same
- If a service contains multiple service option groups, one service option group has the same name as the service, and the others have unique names

Service Options and Service Option Elements

A service option is the most basic element that users can request or subscribe to in the catalog. A service option consists of one or more service option elements. The service options in the Best Practice content have the following service option elements. Your modified catalog can have more or fewer service option elements, depending on its design.

Note: If you are using CA Workflow, verify that the first service option element in a service option is a Text type service option element using plain text. Do not use rich text. Otherwise, no restrictions exist on the number, types, or order of the remaining service option elements.

Short Description

Specifies a plain text field (not rich text) that describes the service being requested or subscribed to.

Use this option to describe the service in cases where rich text or HTML is not processed properly. For example, the workflows use this column to title the email.

Long Description

Specifies a rich text field.

This text describes the service in greater detail and can include a hyperlink to an internal web page containing additional information about the service.

Rate

Specifies the cost of the service option.

Best Practices dictate that consumers understand the cost of the service to the corporation, regardless of whether the request is charged back.

Because the cost structure at your location is unique, all service option elements have been set to a one-time charge. Best practices suggest that determining cost and rate structures depends on a number of factors. In some cases, the rate posted in the catalog is only advisory: The rate reminds users that although they are not charged, the service is not free. In other cases, however, the posted rate is linked to a chargeback policy. In these cases, it is designed to recover the cost of the service. CA Service Accounting is designed for automating the process of tracking service costs.

Service Level

Describes the level of service the user can expect. The user can click the "More Information" link to get a description of the basic levels of service that they can subscribe to. The sample information displayed when you click the "More Info" hyperlink is contained in "sladescription.html" located in the %USM_HOME%\filestore\images\offerings directory. You can change this location, as follows: Use the Service Builder to modify each service option element in your catalog to reference a file in another location.

Note: In this implementation of catalog content, the service level agreement service option element is text only. It includes no service level reporting or enforcement using the text service option element.

Special Instructions

Specifies additional instructions for the user.

Many services require users to specify additional detail information. An example is a "backup production server" service on which you must back up files and specify the backup interval. The instructions tell users to place this information in the notes associated with a request.

Note: You can use the Form service option element type to present custom forms to gather additional information from the requester.

Images

You can optionally associate images with every folder, service and service option. All images reside in %USM_HOME%\filestore\images\offerings.

Images whose size is 32x32 pixels fit best in the catalog.

Images can be in any format suitable for a web browser (.jpg, .bmp, and so on).

Many predefined images exist in this directory. The Best Practice content does not use all of them. You can optionally use these predefined images and add others to meet the needs of your organization. Use images that help users searching for a service to find the service they need.

Category, Class, and Subclass

The first service option element in a service option determines the Category, Class and Subclass for the other items in that row. The Best Practice: Foundation catalog uses several Category/Class/Subclasses which are defined in category.xml. If you are building your catalog "from scratch," you can use any Class/Subclass structure. Because the Category drives associated Workflow processing and other downstream activities, the predefined Category corresponding numeric values must not be changed.

The predefined service option elements reference the predefined category, class and subclass values in the category.xml file. Therefore, if you build your catalog on top of the best practices content, do not *change* the predefined settings in the file. Instead, *add* new categories, classes, or subclasses in the file, if necessary.

Service Specification

When you design your catalog, consider the following service specification factors. These attributes help your customers understand the service.

Attribute Name	Definition
Service Description	Brief description of the service which explains what the service includes
Service Exclusions	Brief clarification regarding what is not included in the service
Service Core Dependencies	Listing of the underlying services and processes that are necessary for this service
Service Options	The various components and options available to users when ordering the service from the catalog

Attribute Name	Definition
Service Hours	The time period during which the service is typically available
Service Maintenance and Planned Down Time	The time period during which the service is typically not available due to scheduled maintenance
Service Availability	The targeted percentage (of the defined Service Hours) during which service is available for requests
Service Owner (Performance Measure Owner)	The person responsible for the service
Service Users	The intended group of requesters for this service
Performance Measures/Descriptions	One or more defined performance measurements for the service fulfillment with a base line target
Key Performance Indicators	The performance measurement which is the primary indicator of the performance of the fulfillment of this service
Key Goal Indicators	The overall company benefit from this service
Data Collection Method/Frequency	An overview of the intended data collection method and frequency. If tools and methods are known, specify them here
Cost Categorization (to Business Unit)	Definition of the cost categorization of the service regarding the following aspects of costs: direct and indirect, capital and operational, fixed and variable, cost type, cost elements, cost units
Charging Policies	The charging policy for this service. The template gives examples both for internal and external providers

Sample Service Specification

This sample server specification illustrates the following costs associated with the "Personal Computer (PC)" service:

- Direct (associated costs allocated directly to the IT organization) for the request of the other vendor software
- Capital for the acquisition of the new PC
- Variable depending on the number of new PC requests

Charges are based on the following elements:

- Internal Service Provider
- Initial setup of the service at the time of SLA signature plus Hardware
- Fixed subscription per year
- Cost of usage per request
- External Service Provider
- Market Standard

Element	Description
Service Name	Personal Computer (PC)
Service Description	New Desktop or Laptop
Service Exclusions	No support, no equipment returns
Service Core Dependencies	Architectural standards, including approved server hardware lists Procurement process for IT infrastructure equipment, including appropriate vendor agreements
Service Options	Options, such as Standard Laptop, Deluxe Laptop, Standard Desktop, Deluxe Laptop
Service Hours	24 hours per day, 7 days per week, 365 days per year Can vary, depending on Service Level selected by customer
Service Maintenance and Planned Down Time	Last Sunday of every month from 2AM - 3AM EST Can vary, depending on Service Level selected by customer
Service Availability	Availability Target: 99% of Service Hours Can vary, depending on Service Level selected by customer

Service Owner (Performance Measure Owner)	John Doe - Director, IT Organization
Service Users	Finance, Marketing, Operations, and Customer Service Organizations
Performance Measures and Descriptions	<p>Acknowledgment of order Number of hours elapsed between the time the user submitted the request and the time the user received acknowledgment of the order Target: Average less than 8 hours</p> <p>Order Fulfillment: Normal Number of days elapsed between the time the user submitted the request and the time the user received acknowledgment that the requested items are available Target: Average less than 7 days</p>
Key Performance Indicators	Number of days elapsed between the time the user submitted the request and the time the vendor notified the user that order was shipped
Key Goal Indicators	<p>Better capacity planning and inventory management through standardized procurement processes</p> <p>Compliance to SLAs by third-party vendors and providers</p> <p>Standardization of computers throughout the organization</p>
Data Collection Method/Frequency	Data is collected for “time of request”, “time of acknowledgment” and “PC available” by feeds from tools used at each event. If feeds are not available, collect the data daily (24h).
Cost Categorization	<p>Direct and Indirect - Direct cost of service Capital and Operational Capital</p> <p>Fixed and Variable - Fixed based for subscription - variable per request</p> <p>Cost Type - Service + Hardware</p> <p>Cost Elements - Hardware + Services Defined in Service Dependencies</p> <p>Cost Units - Per Request + Hardware</p>

Charging Policies	Internal Service Provider - Fixed Setup Price + Hardware External Service Provider - Market Price
-------------------	---------------------------------------------------------------------------------------------------------

Chapter 12: Customizing

This section contains the following topics:

- [Introduction to Customization](#) (see page 275)
- [How to Add Custom Fields to the User Interface](#) (see page 276)
- [Request Status Values](#) (see page 279)
- [How to Customize the Request Status List](#) (see page 280)
- [Category, Class and Subclass Lists](#) (see page 294)
- [Customize the Category, Class and Subclass Lists](#) (see page 295)
- [User and Service Approval List](#) (see page 297)
- [Maintain the User and Service Approval Level List](#) (see page 298)
- [Request and Priority List](#) (see page 299)
- [Typefaces Available for Notes in Requests](#) (see page 304)
- [How to Customize the Typefaces Available for Notes in Requests](#) (see page 305)
- [How to Customize XSL, XML, JavaScript, and Image Files](#) (see page 306)
- [Increase the Number of Values for a Drop-Down Variable](#) (see page 308)
- [Custom Branding](#) (see page 309)
- [Customize the Online Help](#) (see page 330)

Introduction to Customization

You can customize certain features of CA Service Catalog.

Important! As a CA Service Catalog administrator and user, you create, test, and maintain your own individual customizations. Therefore, make careful notes of the customizations you perform, so that you can reference them and repeat them as needed. Doing so is especially when you troubleshoot them and when you upgrade to a new version of CA Service Catalog.

How to Add Custom Fields to the User Interface

On the CA Service Catalog user interface, you can optionally add custom field related to business units, accounts, or users. You can add a new field to meet a custom requirement for your organization or one of your customers. To do so, follow this process:

1. Review the [additional data fields](#) (see page 276) for business units, accounts, or users. By default, these fields exist in the CA Service Catalog database but are not exposed to users.
2. Review the [sample custom.xml file](#) (see page 277) to become familiar with it. This file lists the same additional data fields that exist in the database. You edit this file to expose those fields on the user interface.
3. [Expose the additional data field](#) (see page 278) you want on the user interface by adding a label for the field in the custom.xml file.

Additional Data Fields

The Business Unit, Account, and User schemas in the CA Service Catalog database tables provide additional data fields. By default, these fields do not have labels, meaning that they do not appear on the CA Service Catalog user interface. You can optionally [expose an additional data field](#) (see page 278) on the user interface by adding a label for the field in the [custom.xml file](#) (see page 277).

The additional data fields and their data types follow.

- The additional data fields (and their types) for business units in the `usm_tenant` table follow:
 - data1: nvarchar(32)
 - data2: nvarchar(32)
 - data3: nvarchar(32)
 - data4: nvarchar(64)
 - data5: nvarchar(64)
 - data6: nvarchar(128)
 - data7: nvarchar(128)

- The additional data fields (and their types) for accounts in the usm_account table follow:
data1: nvarchar(32)
data2: nvarchar(32)
data3: nvarchar(32)
data4: nvarchar(64)
data5: nvarchar(64)
data6: nvarchar(64)
data7: nvarchar(128)
- The additional data fields (and their types) for users in the usm_contact_extension table follow:
data1: nvarchar(512)
data2: nvarchar(512)
data3: nvarchar(512)
data4: nvarchar(512)
data5: nvarchar(512)
data6: nvarchar(512)
data7: nvarchar(512)

Sample Custom.xml File

The custom.xml file lists all [additional data fields](#) (see page 276) for CA Service Catalog. You can optionally [expose an additional data field](#) (see page 278) on the CA Service Catalog user interface by adding a label to the field.

The custom.xml file can be different based on the language chosen for the system and is located in a different folder for each language. For example, for English (icusen), the custom.xml file is located in the %USM_HOME%\view\webapps\usm\locale\icusen folder.

A sample custom.xml file follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<shared>
  <account>
    <data1></data1>
    <data2></data2>
    <data3></data3>
    <data4></data4>
    <data5></data5>
    <data6></data6>
    <data7></data7>
  </account>
</shared>
```

```
<tenant>
  <data1></data1>
  <data2></data2>
  <data3></data3>
  <data4></data4>
  <data5></data5>
  <data6></data6>
  <data7></data7>
</tenant>
<user>
  <data1></data1>
  <data2></data2>
  <data3></data3>
  <data4></data4>
  <data5></data5>
  <data6></data6>
  <data7></data7>
</user>
</shared>
```

Expose Additional Data Fields

By default, the [additional data fields](#) (see page 276) for business units, accounts, and users exist in the database but are *not* exposed on the CA Service Catalog user interface. You can optionally expose these fields [to add custom fields to the user interface](#) (see page 276). You can do so to meet a custom requirement for your organization or one of your customers.

To expose an additional data field in the user interface

1. Use an editor, such as Notepad, to edit the [custom.xml file](#) (see page 277) for the language of your system. For example, for English, edit the %USM_HOME%\view\webapps\usm\locale\icusen\custom.xml file.
2. Type the label for the field between the start and end tags for the appropriate field (data1-data7) for the appropriate object: account, business unit (tenant), or user.

This label appears on the user interface to help users identify the purpose of the field.
3. Save the custom.xml file.
4. Verify that the label appears as specified when you view the related object on the GUI. Examples include the associated add, edit and profile pages.

Example: Expose Additional Fields in the User Interface

This example configures the account data1 and account data 5 fields in the custom.xml file to expose Cost Center and Department data on the GUI:

```
<account>
  <data1>Cost Center</data1>
  <data2></data2>
  <data3></data3>
  <data4></data4>
  <data5>Department</data5>
  <data6></data6>
  <data7></data7>
</account>
```

Note: To expose a field without specifying a new label on the user interface, specify a space as the value of the label.

Request Status Values

Each service and service option in a request has a status. In addition, the request has an overall status. CA Service Catalog supplies an extensive list of status values by default. You can [customize](#) (see page 280) (add, change, or hide) status values for the approval and fulfillment phases of the request life cycle, by editing the requestshared.xml file. You can also change the spelling of existing status values. Be careful not to change the meaning of the status values, because business logic in the product is based on these status values.

You maintain the request status values in the requestshared.xml file. This file can be different based on the language chosen for the system and is located in a different folder for each language. For example, for English (icusen), the requestshared.xml file is located in the %USM_HOME%\view\webapps\usm\locale\icusen\request folder.

The request status of the *entire* request is visible on the Pending Actions page. The request statuses of individual items in the request are visible in the Item Status drop-down list on the request-related user interface pages: Request Details, Approve Request, Fulfill Request, and Push Through Request. Updates that you make to the request status values in the requestshared.xml file are reflected in the options that users see on those pages.

How to Customize the Request Status List

You customize (add, delete, edit, or hide) [request status values](#) (see page 279) by editing the requestshared.xml file. To do so, perform these tasks:

1. [Become familiar with the requestshared.xml file](#) (see page 280).
2. Back up the original requestshared.xml file and save it for reference.
3. (Optional) Modify existing status values or [add additional request statuses](#) (see page 286).
4. (Optional) [Hide request statuses](#) (see page 289).
5. (Optional) [Restrict the status changes available for a request item based on its status](#) (see page 291).

You can optionally restrict the status changes available for a request item based on its status. The available status changes appear in the menu options of the Item Status drop-down list on the following request-related user interface pages: Request Details, Approve Request, and Fulfill Request.

By default, all options (all statuses) are available for an item at all times, until the entire request is completed. In other words, you can change the status of request items to any value at any time. However, your organization can optionally restrict the menu options available for a request item based on its status.

6. Test your changes by verifying that they are correctly reflected on the request-related user interface screens.

Note: In the Item Status drop-down list on the request-related user interface pages, the status is designated with an asterisk (*).

Important! After you have added and used additional status numeric values to the default list, do *not* remove them.

Become Familiar with requestshared.xml

Become familiar with the requestshared.xml file, as follows:

- Understand the purpose of the [major sections](#) (see page 281) of the file: request_header, request_item, request_item_approval_action, and request_item_fulfillment_action.
- Understand that the status values in these sections must remain synchronized.
- Understand that the order of the statuses in the status drop-down lists on the GUI matches the order of the statuses in the requestshared.xml file. For example, suppose that the status 800 (Reject) is defined above the status 600 (Approved) in this file. In this case, the Reject status appears above the Approved status in the status drop-down lists on the GUI.
- Review the inline comments and note the *reserved* status values.

- Review the [ranges for custom status values](#) (see page 282) to see which ranges are reserved for specific types of status values.
- Review the [sample sections](#) (see page 282) that illustrate how the settings in the file determine the values of request statuses.

Important! When you edit the `requestshared.xml` file, do *not* modify or delete the opening and closing lines that define the default statuses! Even when you customize statuses, these lines must remain as shown. This requirement applies to both the `<request_item_approval>` and `<request_item_fulfillment>` sections. These lines help ensure proper status behavior when the customizations are not used or are defined incorrectly.

```
- <custom_menu current_status_value="default">
  status_lines
</custom_menu>
```

Major Sections

The major sections of the [requestshared.xml](#) (see page 280) file are as follows:

request_header

Maintains all possible status values for the entire request.

request_item

Maintains all possible status values for a specific item (such as a service option element or service option group) in a request.

request_item_approval_action

Maintains all possible status values for a specific item in a request, when the request has been submitted but has not been approved or rejected.

request_item_fulfillment_action

Maintains all possible status values for a specific item in a request, when the request has been approved but has not yet been fulfilled.

The list of possible status values must be synchronized in the `request_header` and `request_item` sections: They must have the same values with same meaning.

Similarly, every value in the `request_item_approval_action` and `request_item_fulfillment_action` sections must have a matching value in both the `request_header` and `request_item` sections. Thus, the value in the `request_item_approval_action` and `request_item_fulfillment_action` sections must be a complete set or a subset of the values in the `request_header` and `request_item` sections.

Ranges for Custom Status Values

When adding a new request status in the [requestshared.xml file](#) (see page 280), define it within the range specified for the custom statuses, as follows:

- 300 to 399 - custom *submit* statuses
- 500 to 599 - custom *pending approval* status
- 900 to 990 - custom *approved* status

Sample Sections

The following sample sections of the [requestshared.xml file](#) (see page 280) illustrate important settings that control the request status values. In these sections, the ellipses represent omitted lines.

```
<?xml version="1.0" encoding="UTF-8" ?>
...
- <request_header>
  <!-- status values must be synchronized with the status list in request_item, request_item_approval_action
and/or request_item_fulfillment_action -->
...
  <st_1>Pending</st_1>
  <st_2>Completed</st_2>
...
  <st_100>Not Submitted</st_100>
  <st_101>Not Submitted - Cart</st_101>
...
  <!-- 400 to 499 are reserved -->
  <st_400>Pending Approval</st_400>
...
  <!-- 800 to 899 are reserved -->
  <st_800>Approved</st_800>
  <st_801>Approval Not Needed</st_801>
...
  <st_1000>Pending Fulfillment</st_1000>
  <st_1001>Check Availability</st_1001>
...
  <st_1999>Fulfillment Cancelled</st_1999>
  <st_2000>Fulfilled</st_2000>
...
</request_header>
```

```

- <request_item>
  <!-- status values must be synchronized with the status list in request_header, request_item_approval_action
and/or request_item_fulfillment_action -->
  ...
  <st_1>Pending</st_1>
  <st_2>Completed</st_2>
  ...
  <st_100>Not Submitted</st_100>
  <st_101>Not Submitted - Cart</st_101>
  ...
  <!-- 400 to 499 are reserved -->
  <st_400>Pending Approval</st_400>
  ...
  <!-- 800 to 899 are reserved -->
  <st_800>Approved</st_800>
  <st_801>Approval Not Needed</st_801>
  ...
  <st_1000>Pending Fulfillment</st_1000>
  <st_1001>Check Availability</st_1001>
  ...
  <st_1999>Fulfillment Cancelled</st_1999>
  <st_2000>Fulfilled</st_2000>
  ...
</request_item>

- <request_item_approval_action>
  <!-- status values must be synchronized with the status list in request_header and request_item -->
  <!-- A "default" value for the attribute "current_status_value" indicates these statuses are listed by default in the
"item status" menu if no other custom statuses are defined -->

<custom_menu current_status_value="default">
  <!-- 400 to 499 are reserved -->
  <st_400 statval="400"/>

  <!-- 500 to 599 can be used for custom pending approval status -->
  <!-- 600 to 699 are reserved -->
  <!-- 700 to 799 can be used for custom rejected status -->
  <!-- 800 to 899 are reserved -->
  <st_800 statval="800"/>
  <!-- 900 to 999 can be used for custom approved status -->
  <st_600 statval="600"/>
</custom_menu>

```

```
<custom_menu current_status_value="800">
  <!-- 400 to 499 are reserved -->
  <st_800 statval="800"/>
  <st_999 statval="999"/>
  <!-- 900 to 999 can be used for custom approved status -->
  <st_600 statval="600"/>
</custom_menu>
...
</request_item_approval_action>
<request_item_stuck_approval_action>
<custom_menu current_status_value="default">
  <!-- 400 to 499 are reserved -->
  <st_400 statval="400"/>
  <!-- 500 to 599 can be used for custom pending approval status -->
  <!-- 600 to 699 are reserved -->
  <!-- 700 to 799 can be used for custom rejected status -->
  <!-- 800 to 899 are reserved -->
  <st_800 statval="800"/>
  <!-- 900 to 999 can be used for custom approved status -->
  <st_600 statval="600"/>
</custom_menu>
...
<custom_menu current_status_value="200">
  <!-- 400 to 499 are reserved -->
  <st_200 statval="200"/>
  <st_999 statval="999"/>
  <!-- 900 to 999 can be used for custom approved status -->
  <st_600 statval="600"/>
</custom_menu>
</request_item_stuck_approval_action>
...
<request_item_stuck_fulfillment_action>
  <!-- status values must be synchronized with the status list in request_header
and request_item -->
  <!-- A "default" value for the attribute "current_status_value" indicates these
statuses are listed by default in the "item status" menu if no other custom statuses are defined -->
  <!-- The order of the statuses that appear in the status drop-down lists on the UI
are based on the sequence of the status codes added here
For ex: because status 1999 is defined above 2000 in this file, then
status 1999 appears above status 2000 in the status drop-down lists on the UI
-->
  <custom_menu current_status_value="default">
    <st_1999 statval="1999"/>
    <st_2000 statval="2000"/>
  </custom_menu>
```

```
<custom_menu current_status_value="1000">
    <st_1000 statval="1000"/>
    <st_1999 statval="1999"/>
    <st_2000 statval="2000"/>
</custom_menu>

<custom_menu current_status_value="1001">
    <st_1001 statval="1001"/>
    <st_1999 statval="1999"/>
    <st_2000 statval="2000"/>
</custom_menu>

<custom_menu current_status_value="1002">
    <st_1002 statval="1002"/> <!-- if this value changes, synchronize
with items located in section uapm_url below -->
    <st_1999 statval="1999"/>
    <st_2000 statval="2000"/>
</custom_menu>

<custom_menu current_status_value="1003">
    <st_1003 statval="1003"/>
    <st_1999 statval="1999"/>
    <st_2000 statval="2000"/>
</custom_menu>

...

<custom_menu current_status_value="1007">
    <st_1007 statval="1007"/>
    <st_1999 statval="1999"/>
    <st_2000 statval="2000"/>
</custom_menu>

<custom_menu current_status_value="1008">
    <st_1008 statval="1008"/>
    <st_1999 statval="1999"/>
    <st_2000 statval="2000"/>
</custom_menu>

...

</request_item_stuck_fulfillment_action>

...
</shared>
```

Add an Additional Request Status

You can [customize the request status list](#) (see page 280) by adding additional request statuses for one of several purposes not covered by the default statuses. One common purpose is for approval or rejection of a request by a specific department, for example, the Finance department.

Follow these steps:

1. Use an editor, such as Notepad, to edit the appropriate requestshared.xml file for the language of your system. For example, for English, edit the file in the %USM_HOME%\view\webapps\usm\locale\icusen\request folder.
2. Add an additional line, including the number and text for the new status to the following sections: <request_header> and <request_item>.
3. Select an unused numeric status value in the appropriate [range for custom status values](#) (see page 282) for the status you are adding. An example follows:

```
<st_500>Pending Financial Approval</st_500>
...
<st_700>Rejected by Financial Approver</st_700>
...
<st_900>Approved by Financial Approver</st_900>
...
```

Note: If possible, limit the text of the status value to 40 characters. Text longer than 40 characters can be truncated in the drop-down status menu lists and request status fields. In such cases, the entire text string is displayed to catalog users *only* in the tooltip text that appears when users mouseover request status fields.

4. Copy that line to the custom section or sections where you want them to appear. Examples include <request_item_approval>, <request_item_fulfillment>, <request_item_stuck_approval_action>, and <request_item_stuck_fulfillment_action>.
5. Delete the text from the line you copied and modify the line to include the statval="value" expression.

An example for the previous step follows:

```
<st_500 statval="500"/>
...
<st_700 statval="700"/>
...
<st_900 statval="900"/>
...
```

Note: This technique is illustrated in greater detail in the Example section that follows this section.

6. Save the requestshared.xml file.
7. Test your changes by verifying that they are correctly reflected on the request-related user interface screens (the Request Details, Approve Request, and Fulfill Request screens).

Example: Add New Approval Statuses

To add approval statuses 500, 700, and 900, all related to financial approval, add the new lines for these statuses to the request_header, request_item, and request_item_approval_action sections of the requestshared.xml file. Examples follow, in **bold**.

Specify the numeric value and text in the request_header and request_item sections, and specify only the numeric value (without the text) in the request_item_approval_action section.

```
<?xml version="1.0" encoding="UTF-8" ?>
...
- <request_header>
  <!-- status values must be synchronized with the status list in request_item, request_item_approval_action
and/or request_item_fulfillment_action -->
  <st_1>Pending</st_1>
  <st_2>Completed</st_2>
  ...
  <!-- 400 to 499 are reserved -->
  <st_400>Pending Approval</st_400>
  <!-- 500 to 599 can be used for custom pending approval status -->
  <st_500>Pending Financial Approval</st_500>
  <!-- 600 to 699 are reserved -->
  <st_600>Rejected</st_600>
  <!-- 700 to 799 can be used for custom rejected status -->
  <st_700>Rejected by Financial Approver</st_700>
  <!-- 800 to 899 are reserved -->
  <st_800>Approved</st_800>
  <st_801>Approval Not Needed</st_801>
  <!-- 900 to 990 can be used for custom approved status -->
  <st_900>Approved by Financial Approver</st_900>
  <!-- 991 to 999 are reserved -->
  <st_999>Approval Done</st_999>
  ...
</request_header>
- <request_item>
  <!-- status values must be synchronized with the status list in request_header, request_item_approval_action
and/or request_item_fulfillment_action -->
  <st_1>Pending</st_1>
  <st_2>Completed</st_2>
```

```
...
<!-- 400 to 499 are reserved -->
<st_400>Pending Approval</st_400>
<!-- 500 to 599 can be used for custom pending approval status -->
<st_500>Pending Financial Approval</st_500>
<!-- 600 to 699 are reserved -->
<st_600>Rejected</st_600>
<!-- 700 to 799 can be used for custom rejected status -->
<st_700>Rejected by Financial Approver</st_700>
<!-- 800 to 899 are reserved -->
<st_800>Approved</st_800>
<st_801>Approval Not Needed</st_801>
<!-- 900 to 990 can be used for custom approved status -->
<st_900>Approved by Financial Approver</st_900>
<!-- 991 to 999 are reserved -->
<st_999>Approval Done</st_999>
...
</request_item>
- <request_item_approval_action>
  <!-- status values must be synchronized with the status list in request_header and request_item -->
  <!-- A "default" value for the attribute "current_status_value" indicates these statuses will be listed by default in
the "item status" menu if no other custom statuses are defined -->
  <custom_menu current_status_value="default">
    <!-- 400 to 499 are reserved -->
    <!-- 500 to 599 can be used for custom pending approval status -->
    <st_500 statval="500"/>
    <!-- 600 to 699 are reserved -->
    <!-- 700 to 799 can be used for custom rejected status -->
    <st_700 statval="700"/>
    <!-- 800 to 899 are reserved -->
    <st_800 statval="800">Approve</st_800>
    <!-- 900 to 999 can be used for custom approved status -->
    <st_900 statval="900"/>
  ...
```


Hide Request Statuses

The default list of request statuses can include more options than you need for certain categories. In such cases, you can decide to [customize the request status list](#) (see page 280) by hiding some of the values in that category. Consequently, users do not see these options on the GUI when they handle requests pending action. Thus, they do not need to sort through status values that do not apply in your organization.

To hide request statuses

1. Use an editor, such as Notepad, to edit the appropriate requestshared.xml file for the language of your system. For example, for English, edit the file in the %USM_HOME%\view\webapps\usm\locale\icusen\request folder.
2. Decide which status lines you want to hide; that is, decide which statuses do not apply in your organization.
3. Edit the line in the <request_header> and <request_item> sections for each status that you want to hide. Enter the comment characters before and after the original expression.

For example to *hide* the Ordered status on the request-related pages, enter the comment characters before and after the original expression. These comment characters appear in **bold** in the following line:

```
<!--<st_1004>Ordered</st_1004-->
```

In contrast, the following line makes the Ordered status *visible* on the request-related user interface screens:

```
<st_1004>Ordered</st_1004>
```

4. Hide the corresponding lines in all other sections that use it, such as the <request_item_approval> or <request_item_fulfillment> section.

For example, to *hide* the Ordered status on the request-related pages, enter the comment characters before and after the original expression. These comment characters appear in **bold** in the following line:

```
<!--<st_1004 statval="1004"/>-->
```

In contrast, the following line makes the Ordered status *visible* on the request-related user interface screens:

```
<st_1004 statval="1004"/>
```

Note: Hide the exact same lines in all relevant sections of the file. Doing so is required for the status to appear correctly in the user interface.

5. Save the requestshared.xml file.
6. Test your changes by verifying that they are correctly reflected on the following request-related pages: Request Details, Approve Request, and Fulfill Request.

Example: Hide Request Statuses

To hide certain default fulfillment-related statuses, enter the comment characters before and after the original expression, as shown in **bold** in this example. Enter the comment characters in the `request_header`, `request_item`, and `request_item_fulfillment_action` sections of the `requestshared.xml` file.

In this example, *before* the comment markers are added, the following statuses are visible on the following request-related pages: Ordered, Shipped, Received, Order Cancelled, Staged, and Configured. *After* the comment markers are added, the following statuses are visible on those pages: Ordered, Shipped, and Configured.

```
- <request_header>
...
  <st_1004>Ordered</st_1004>
  <st_1006>Shipped</st_1006>
  <!--<st_1007>Received</st_1007-->
  <!--<st_1008>Order Cancelled</st_1008-->
  <!--<st_1017>Staged</st_1017-->
  <st_1019>Configured</st_1019>
...
</request_header>

- <request_item>
...
  <st_1004>Ordered</st_1004>
  <st_1006>Shipped</st_1006>
  <!--<st_1007>Received</st_1007-->
  <!--<st_1008>Order Cancelled</st_1008-->
  <!--<st_1017>Staged</st_1017-->
  <st_1019>Configured</st_1019>
...
</request_item>

- <request_item_fulfillment_action>
...
  <custom_menu current_status_value="default">
...
  <st_1004 statval="1004"/>
  <st_1006 statval="1006"/>
  <!--<st_1007 statval="1007"/-->
  <!--<st_1008 statval="1008"/-->
  <!--<st_1017 statval="1017"/-->
  <st_1019 statval="1019"/>
...
</shared>
```

Restrict the Status Changes Available for a Request Item Based on its Current Status

You can optionally [customize the request status list](#) (see page 280) by restricting the status changes available for a request item based on its current status. For example, suppose that when an item is approved (Approved status), you no longer want users to be able to change the status *except* to a fulfillment-related status. In this case, you can configure the Item Status drop-down list to display *only* fulfillment-related options for items whose status is approved.

To restrict the status changes available for a request item based on its status

1. Use an editor, such as Notepad, to edit the appropriate requestshared.xml file for the language of your system. For example, for English, edit the file in the %USM_HOME%\view\webapps\usm\locale\icusen\request\requestshared.xml folder.
2. Locate the section of the file in which you want to restrict the available changes for one or more status values.

You can restrict status changes in any section *except* the <request_item> and <request_header> sections.

3. Decide which status you want to restrict and the statuses to which you permit it to be changed.

The list of all existing status values appears under the following line:

```
- <custom_menu current_status_value="default">
```

4. [Add an additional request status](#) (see page 286) to permit in your list, if necessary. The statuses that you want to permit must exist already.
5. Locate the custom menu section and complete the following. By default, this section is indented and commented out, as follows:

```
-<!--
                                <custom_menu current_status_value="400">
                                    <st_400 statval="400"/>
                                    <st_600 statval="600"/>
                                </custom_menu>
-->
```

- a. Delete the opening and closing comment lines of this section. The new section appears as follows:

```
<custom_menu current_status_value="400">
    <st_400 statval="400"/>
    <st_600 statval="600"/>
</custom_menu>
```

The lines are now activated rather than being commented out.

- b. Verify that the value in the `current_status_value="nnn"` expression in the first line of this section matches the status value that you want to restrict.

For example, in the previous step, 400 corresponds to the Pending Approval status. Therefore, the status values shown appear on request-related pages when the status value is Pending Approval. If you want to restrict a different status, replace the current value with your new value.

- c. Verify that the value in the `current_status_value="nnn"` expression is defined in one of the `<st_nnn statval=..."` lines, as shown for Pending Approval in the previous example.

- d. Copy and paste the additional status or statuses to which you want to allow the status to be changed. You can copy and paste it from the list of status values earlier in the section.

For example, in the `<request_item_approval>` section, copy and paste the new `<st_801..."` line to the `custom_menu` section for Pending Approval, as follows:

```
<custom_menu current_status_value="400">
    <st_400 statval="400"/>
    <st_600 statval="600"/>
    <st_801 statval="801"/>
</custom_menu>
```

This action adds the Approval Not Needed status to the statuses to which items in Pending Approval status can be changed.

6. Use the previous steps as a model to restrict status changes for another status in the same section of requestshared.xml file, if necessary. Use these guidelines:
 - a. Copy the entire custom_menu element and its children.
 - b. Paste it after the element that you updated.
 - c. Modify the newly copied element.
 - d. Modify existing custom_menu element and children, if necessary. For example, in the <request_item_fulfillment> section, suppose you want to restrict items in Pending Fulfillment status to be changed to either Fulfillment Cancelled or Fulfilled. In that case, modify the existing custom_menu element as follows:

```
<custom_menu current_status_value="1000">
  <st_1000 statval="1000"/>
  <st_1999 statval="1999"/>
<st_2000 statval="2000"/>
</custom_menu>
```

7. Save the requestshared.xml file.
8. Test your changes by verifying that they are correctly reflected on the request-related user interface pages (the Request Details, Approve Request, and Fulfill Request pages).

You have restricted the status changes available for a request item based on its current status.

Category, Class and Subclass Lists

Each service option in the catalog has a category, class and subclass assigned to it. CA Service Catalog assigns a value to each category, class and subclass in the category.xml file.

Each <option> section in the category.xml file represents a separate category and contains one or more <class> sections. Moreover, each of these sections contains one or more <subclass> sections.

You can optionally [customize the category, class and subclass lists](#) (see page 295) by changing the values or by adding new values to meet the needs of your organization or customer.

The category.xml file can be different based on the language chosen for the system and is located in a different folder for each language. For example, for English (icusen), the category.xml file is located in the %USM_HOME%\view\webapps\usm\locale\icusen\billing folder.

The following are sample sections of the category.xml file, with ellipses shown to represent omitted lines:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!--WARNING: THE VALUE ATTRIBUTE CAN BE CHANGED BUT THEY MUST BE UNIQUE WITHIN ITS
OWN NODE LEVEL, FOR EXAMPLE, OPTION "NONE" HAS A VALUE OF "-1",
THEREFORE ANY OTHER OPTIONS LIKE "SOFTWARE" CANNOT HAVE A VALUE OF "-1".-->
<categories>
  <category>
    <option value="-1" name="None">
      <class value="-1" name="None">
        <subclass value="-1" name="None" />
      </class>
    </option>
    <option value="0" name="Software">
      <class value="10" name="Office">
        <subclass value="10" name="Microsoft" />
        <subclass value="99" name="Other" />
      </class>
      ...
    </option>
    <option value="1" name="Hardware">
      <class value="10" name="IT">
        <subclass value="10" name="Desktop" />
        <subclass value="20" name="Laptop" />
        <subclass value="30" name="Monitor" />
        <subclass value="40" name="Memory" />
        <subclass value="50" name="Printer" />
        <subclass value="60" name="Server" />
        <subclass value="70" name="Storage" />
        <subclass value="999" name="Other" />
      </class>
    </option>
  </category>
</categories>
```

```

        </class>
        ...
    </option>
    <option value="2" name="Service">
        <class value="10" name="IT">
            <subclass value="10" name="Application" />
            <subclass value="20" name="Audit" />
            <subclass value="30" name="Data" />
            <subclass value="40" name="Education" />
            <subclass value="50" name="Email" />
            <subclass value="60" name="Incident" />
            <subclass value="70" name="Knowledge" />
            <subclass value="80" name="Security" />
            <subclass value="90" name="SLA" />
            <subclass value="100" name="Labor" />
            <subclass value="999" name="Other" />
        </class>
        ...
    </option>
    <option value="3" name="Other">
        <class value="10" name="IT">
            <subclass value="99" name="Other" />
        </class>
        ...
    </option>
</category>
</categories>

```

Customize the Category, Class and Subclass Lists

Each service option in the catalog has a predefined [category, class and subclass](#) (see page 294) assigned to it. You can optionally customize the category, class, and subclass values: You can update the existing values or add new values to meet the needs of your organization or customer.

Note: After you add a category, class or subclass value in the category.xml file, do *not* remove it. Also, be careful not to change the meaning of the category values, because business logic in the product is based on the category values.

To add or change an additional category, class, or subclass

1. Review the inline comments in the file. Verify that synchronized sections of the file remain synchronized. Verify that you do not use, certain status values.
2. Use an editor, such as Notepad, to edit the appropriate category.xml file for the language of your system. For example, for English, edit the %USM_HOME%\view\webapps\usm\locale\icusen\billing\category.xml file.

3. Add an additional line or section for the category, class, or subclass you want to add. Select an unused numeric value for the category, class, or subclass you are adding.

Note: To add a new category, add a new “option” section containing at least one class and subclass. To add a new class, add a new “class” section containing at least one subclass.

Use a unique numeric value within the list of related objects. For example, suppose you add a new class to the Other category. In that case, you cannot use a value of 10, because the IT class already uses that value.

4. Update any existing values as needed; do *not* to use the same value twice.
5. Save the category.xml file and test by using the Service Builder user interface screens.

Example: Add a New Subclass

To add a new subclass named “Mouse” to the IT class of the Hardware category, modify the category.xml file with the following lines in **bold**:

```
<option value="1" name="Hardware">
  <class value="10" name="IT">
    <subclass value="10" name="Desktop" />
    <subclass value="20" name="Laptop" />
    <subclass value="30" name="Monitor" />
    <subclass value="40" name="Memory" />
    <subclass value="50" name="Printer" />
    <subclass value="60" name="Server" />
    <subclass value="70" name="Storage" />
    <subclass value="71" name="Mouse" />
    <subclass value="999" name="Other" />
  </class>
  ...
</option>
```


User and Service Approval List

Each user is assigned an approval level, in its user profile. Each service that requires approval is also assigned an approval level, in its service definition.

When a service uses the “System approval process,” the approver requires an approval level equal to or greater than the approval level of the service. Otherwise, the approver cannot approve or reject the service.

The approval level values are maintained in a file named `approval_shared.xml`. This file can be different based on the language chosen for the system and is located in a different folder for each language. For example, for English (icusen), the `approval_shared.xml` file is located in the `%USM_HOME%\view\webapps\usm\locale\icusen` folder.

You can add and update the list of approval levels in the `approval_shared.xml` file. After you add an approval level to the file, do not remove it.

The following is the contents of the `approval_shared.xml` file:

```
<?xml version="1.0" encoding="UTF-8"?>
<shared>
  <approval_level>
    <option value=0>Level 0</option>
    <option value=10>Level 10</option>
    <option value=20>Level 20</option>
    <option value=30>Level 30</option>
    <option value=40>Level 40</option>
    <option value=50>Level 50</option>
  </approval_level>
</shared>
```

Note: For more details on approval processes, see the *Administration Guide*.

Maintain the User and Service Approval Level List

You maintain the [approval levels for users and services](#) (see page 297) in a file named `approval_shared.xml`. You can optionally add or change the values in this file to customize it to meet the needs of your organization.

Note: After you add an approval level to the file, do not remove it.

To maintain the user and service approval level list

1. Edit the appropriate `approval_shared.xml` file for the language of your system, using an editor, such as Notepad. For example, for English, edit the `approval_shared.xml` file in the `USM_HOME%\view\webapps\usm\locale\icusen` folder.
2. Add an additional line for the approval level that you want to add. Select an unused numeric value for the approval level you are adding.
3. (Optional) Update an existing name or value in the file.
4. Save the `approval_shared.xml` file.
5. Verify that the new approval level appears as an option when you edit user profiles and service definitions on the product interface.

You have maintained the approval levels for users and services.

Example: Add a New Approval Level

This example uses the bold line in the following `approval_shared.xml` file to add a new approval level whose name is Director and whose value is 60:

```
<?xml version="1.0" encoding="UTF-8"?>
<shared>
  <approval_level>
    <option value=0>Level 0</option>
    <option value=10>Level 10</option>
    <option value=20>Level 20</option>
    <option value=30>Level 30</option>
    <option value=40>Level 40</option>
    <option value=50>Level 50</option>
    <option value=60>Director</option>
  </approval_level>
</shared>
```

Request and Priority List

Every request has a priority assigned to it. CA Service Catalog supplies predefined priority values in the requestinfoshared.xml file. You can add or change the values in this file. You can also use this file to specify which user roles can assign specific priority values to requests. For example, you can add a new priority value named Immediate that only the Service Delivery role can assign to a request.

Note: After you add a new priority value to the requestinfoshared.xml file, do *not* remove it.

The requestinfoshared.xml file can be different for each language and is located in a different folder for each language. For example, for English (icusen), the requestinfoshared.xml file is located in the %USM_HOME%\view\webapps\usm\locale\icusen\request folder.

The following are sample lines from the requestinfoshared.xml file; the ellipses represent omitted lines:

```
<?xml version="1.0" encoding="UTF-8"?>
<shared>
  ...
  <priority_levels>
    <priority_1 propval="1">High</priority_1>
    <priority_2 propval="2">Medium-High</priority_2>
    <priority_3 propval="3">Medium</priority_3>
    <priority_4 propval="4">Medium-Low</priority_4>
    <priority_5 propval="5">Low</priority_5>
  </priority_levels>
  <priority_level_roles>
    <levels role="default">
      <level propval="1" />
    <level propval="2" />
      <level propval="3" defaultSel="true"/>
      <level propval="4" />
      <level propval="5" />
    </levels>
  </priority_level_roles>
  ...
</shared>
```

The [priority levels](#) (see page 300) section of the request and priority list in the requestinfoshared.xml file defines the numeric and text values for each priority

Priority Levels

The <priority_levels> section of the [request and priority list](#) (see page 299) in the requestinfoshared.xml file defines the numeric and text values for each priority. Each <levels> section defines those priority values that are available to the role code specified in the role attribute. The “default” role specification is used when no section exists for the role of the user.

The priority list appears in the order specified in the <priority_levels> section, regardless of role. You can use the defaultSel attribute to specify the default value for a new request according to role. The following table lists the roles and codes:

Role	Code
Catalog User	catalogenduser
Request Manager	requestmanager
Catalog Administrator	catadministrator
End User	enduser
SMA End User	smaenduser
Administrator	administrator
Service Manager	servicemanager
Super Business Unit Administrator	stadministrator
Service Delivery Administrator	spadministrator

You can edit this file to add values or change the spelling of existing values.

Suppose a request uses a priority value that is *not* available to the role of the user editing the request. In that case, the user sees that priority in the list of priority values. Conversely, suppose the request is set to another priority that *is* available the role of the user editing the request. In that case, the user can see *only* the priorities available to its role.

Example: Customizations for the `requestinfoshared.xml` File

If the Catalog End User role does not include priority 1 (High), a user who has that role does not see High listed in the priority list. Moreover, that user cannot set the priority of a request to High.

Suppose the following occur:

- A Request Manager who can use all the status values later sets the priority of the request to High
- A user with the Catalog End User role later edits the request

In this case, the status of High does appear in the priority list.

Thus, administrators *can* configure the product to prevent a certain role from using a particular priority value. However, administrators cannot prevent users in that role from viewing and editing their requests when another user has set the priority.

How to Maintain the Request Priority List

The [priority levels](#) (see page 300) section of the [request and priority list](#) (see page 299) in the `requestinfoshared.xml` file defines the numeric and text values for each priority. If your organization has a custom need that the predefined priority levels do not meet, do one or both of the following:

- [Add a new priority level for a specific role](#) (see page 303)
- [Add a new priority level for multiple roles](#) (see page 302)

Add a New Priority Level for Multiple Roles

If necessary for your organization, you can add a new [priority level](#) (see page 300) to the predefined priority levels. You can add a new priority level for multiple roles (as explained in this topic) or [for a specific role only](#) (see page 303).

To add a new priority level for multiple roles

1. Edit the requestinfoshared.xml file for the language of your system, using an editor, such as Notepad. For example, for English, edit the %USM_HOME%\view\webapps\usm\locale\icusen\request\requestinfoshared.xml file.
2. Add a new line in the priority_levels section for the priority you want to add. Specify a unique numeric value for the new priority level.

The priority values are listed in the user interface in the order that they appear in this section of the file.

3. Do *one* of the following:
 - Add a line in the levels section for each role that you permit to use the new priority.
 - Add a line in the levels section for the role. The line makes the new priority available to all users who do not have a role-specific priority list.
4. Save the file.
5. Log in to CA Service Catalog as a user with the role that you modified and verify your updates on the request-related pages.

Example: Add a New Priority for All Roles

This example adds the following **bold** line to the requestinfoshared.xml file. This example adds a new priority named “Urgent” and makes it available to all users who do not have a role-specific priority list.

```
<priority_levels>
<bpriority_6 propval="6">Urgent</priority_6>
<priority_1 propval="1">High</priority_1>
<priority_2 propval="2">Medium-High</priority_2>
<priority_3 propval="3">Medium</priority_3>
<priority_4 propval="4">Medium-Low</priority_4>
<priority_5 propval="5">Low</priority_5>
</priority_levels>
<priority_level_roles>
  <levels role="default">
    <level propval="1" />
  <level propval="2" />
    <level propval="3" defaultSel="true"/>
    <level propval="4" />
    <level propval="5" />
    <blevel propval="6" />
  </levels>
</priority_level_roles>
```

Add a New Priority Level for a Specific Role

If necessary for your organization, you can add a new [priority level](#) (see page 300) to the predefined priority levels. You can add a new priority level for a specific role only (as explained in this topic) or [for multiple roles](#) (see page 302).

To add a priority list for a specific role

1. Edit the requestinfoshared.xml file for the language of your system, using an editor such as Notepad. For example, for English, edit the %USM_HOME%\view\webapps\usm\locale\icusen\request\requestinfoshared.xml file.
2. Add a new level section for the affected role.
3. Do *all* of the following in that section:
 - Specify the role code in the role attribute
 - Include only the lines from the priority_levels section that you want users in the role to see
 - Specify the default priority for new requests by using the defaultSel attribute
4. Save the file.
5. Log in to CA Service Catalog as a user with the role that you modified and verify your updates on the request-related pages.

Example: Add a New Priority Level for a Specific Role

This example adds a new priority list for users with the Catalog User role. This example sets the default priority to Medium-Low and does *not* allow users to set the priority to High. This example achieves these goals by adding the new section shown in **bold** in the following sample requestinfoshared.xml file:

```
<priority_levels>
<priority_1 propval="1">High</priority_1>
<priority_2 propval="2">Medium-High</priority_2>
<priority_3 propval="3">Medium</priority_3>
<priority_4 propval="4">Medium-Low</priority_4>
<priority_5 propval="5">Low</priority_5>
</priority_levels>
<priority_level_roles>
  <levels role="default">
    <level propval="1" />
  <level propval="2" />
    <level propval="3" defaultSel="true"/>
    <level propval="4" />
    <level propval="5" />
  </levels>
  <levels role="catalogenduser">
<level propval="2" />
    <level propval="3" />
    <level propval="4" defaultSel="true"/>
    <level propval="5" />
  </levels>
</priority_level_roles>
```

Typefaces Available for Notes in Requests

Users can add notes to requests by accessing the Request Details page and clicking Add in the Notes section. The Add Notes dialog appears and presents several type faces and type sizes as options. For these notes, the default typeface is Arial, and the default type size is 8-point. In addition, users can apply several formatting and highlighting options to these notes.

By default, all supported type faces are enabled, meaning that the Add Notes dialog displays all type faces listed in the section of requestshared.xml. Administrators can optionally [customize](#) (see page 305) (limit or expand) the typefaces that appear to users in the drop-down list of the dialog.

Users can select a typeface in the drop-down list that the local computer being used to display or print the request does not support. In that case, the typeface changes to the default typeface, Arial.

How to Customize the Typefaces Available for Notes in Requests

You can optionally limit or increase the [typefaces available to users when they add notes in requests](#) (see page 304). You can do both activities to help standardize the appearance of these notes or to meet other requirements.

To customize the typefaces available to users for notes in requests

1. Open the requestshared.xml file and move to the section of the file.
2. Leave the type faces that you want to be available to users for notes in request. Comment out the type faces that you do not want to appear in the dialog.

Use the comment prefix expression (<!--) and suffix expression (-->) to enclose any line whose font you want to exclude from the Add Notes dialog.

For example, to comment out the Courier New and Bookman Old Style type faces, modify their lines as follows:

```
<!--<courier_new>Courier New</courier_new-->
```

```
<!--<bookman_old_style>Bookman Old Style</bookman_old_style-->
```

The fonts you left remain available to users for notes in requests. Similarly, any fonts that you commented become unavailable.

3. Do the following to add a new typeface to the list that appears in the drop-down list in the dialog: Enter a new line and specify the new typeface. Use the following convention: If the font name is X Y, use the format <x_y>X Y</x_y>.

For example, to add a typeface named my company font, add the following line to the section:

```
<my_company_font>my company font</my_company_font>
```

The fonts you added become available to users for notes in requests.

4. Save and close the requestshared.xml file.
The Catalog system saves the file.
5. Do the following to help ensure that any font you added or did not comment out is available for display or printing purposes: Verify that the local computer being used to display or print the request supports the font.
6. Verify your changes by adding a note to a request and reviewing the available typefaces.

You have customized the typefaces available to users for notes in requests.

How to Customize XSL, XML, JavaScript, and Image Files

CA Service Catalog includes several hundred XSL, XML, JavaScript, and image files. Together, they are used to form every page and every page element in the product. Each file represents one page or a part of a page, such as a dialog, menu option, form field control, message, or picture.

Every file is named intuitively to illustrate its function. You can optionally customize any of these files to meet your requirements. To customize XSL, XML, JavaScript, and image files, follow this process:

1. Determine the specific page or part of a page that you want to customize.
 2. Locate the file whose name matches the element you want to change. For example:
 - To modify the configuration information of any of the integrated products, locate the `toolsconfig.xml` file.
 - To modify states of request lifecycle, locate the `requestshared.xml` file.
 - To modify the messages that appear when a user tests the connection for a new administration configuration setting, locate the `toolsconfig.js` and `toolsconfig.xsl` files.
 - To modify the edit button of the Administration, Configuration page, locate the `modify.gif` and `toolsconfig.xsl` files.
 - [Modify the request status list](#) (see page 280) by editing the `requeststatus.xml` file.
- Note:** For information about customizing forms using Javascript and other methods, see the *Administrator Guide*.
3. Open the file, review its contents, and verify that it controls the element or behavior that you want to change.
 4. Using the table at the end of these steps as a reference, copy the file from its original location to the custom location.
 5. Modify the file to meet your requirements.
 6. If you customized a JavaScript or image file, perform this step; otherwise, skip it.
 - a. Copy the customized JavaScript file to the `\FileStore\custom\explorer\scripts` folder.
 - b. Copy the customized images to the `\FileStore\custom\images` folder.

- c. Locate the XSL file in the custom location in which the JavaScript or image file is used.
- d. Update this XSL file to specify the new custom path name of the JavaScript or image file. To do so, prepend "FileStore/" to the relative path of the JavaScript or image file. Use the following example as a model:

```
<script src="FileStore/custom/explorer/scripts/custom_form_example.js"></script>
```

This action is required because the XSL file references the [filestore](#) (see page 187) location for the customized script files.

Important! If you are using multiple Service View computers, verify that the filestore is shared among *all* of them.

7. Clear the %USM_HOME%\view\translets folder on all Service View computers: Delete all files in this folder, but do *not* delete the folder itself.
8. Restart all Service View computers.
9. Verify that the changes are working in CA Service Catalog as you intended.

In the following table, the parent folder is %USM_HOME%/view/webapps/usm. The filestore folder is %USM_HOME%/filestore. The folder entries, such as /explorer and /custom/explorer, are subfolders under the parent and filestore folders.

File Type	Original Location in Parent Folder	Custom Location in Filestore Folder
XSL	/explorer	/custom/explorer
XSL	/explorer/request	/custom/explorer/request
XML	/locale/icusen*	/custom/locale/icusen*
XML	/locale/icusen*/request	/custom/locale/icusen*/request
image	/images	/custom/images
image	/images/billing	/custom/images/billing
JS	/explorer/scripts	/custom/explorer/scripts

*The folder name *icusen* applies to English-language implementations only. If you are using a non-English implementation, your locale-specific folder name is different. In such cases, use your locale-specific folder name instead of *icusen*.

Increase the Number of Values for a Drop-Down Variable

When an administrator adds a query runtime variable that appears as a drop-down list to users, the limit for the number of values in the list is 1000. If the report query returns more than 1000 values, the system truncates these additional values. Consequently, the user cannot view them in the drop-down list. If necessary, use this procedure to increase the number of values that appear in the drop-down list to be greater than 1000.

Note: For details about adding query runtime variables, see the *Administration Guide*.

Increase the number of values for a drop-down variable

1. Verify that your implementation has set up a filestore, [a single location for shared files](#) (see page 187). If necessary, set up a filestore.
2. Copy the `reportsgenericgetvariables.xml` file from its *parent* folder (`%USM_HOME%\View\webapps\usm\explorer\reports`) to the *filestore* folder. Follow the same steps as for [customizing XSL, XML, JavaScript, and image files](#) (see page 306).
3. Open the `reportsgenericgetvariables.xml` file in the filestore and locate the following line:

```
<input type="hidden" name="Args" value="1000"/> <!--1-->
```
4. Increase 1000 to the value you want.
5. Save the file.
6. Complete the remaining steps for [customizing XSL, XML, JavaScript, and image files](#) (see page 306) that apply to the `reportsgenericgetvariables.xml` file.
7. Run a report to test the increased limit and verify the results.

You have increased the number of values for a drop-down variable.

Custom Branding

As an administrator, you can customize the look-and-feel of the CA Service Catalog UI. The main categories of look-and-feel elements that you can customize are the following:

- Logos are image files that uniquely identify a company, business unit, or super business unit.

These logos include the [login logo](#) (see page 311), [global logo](#) (see page 312), and [business unit logo](#) (see page 313).

For each business unit, you can optionally specify a *business unit* logo. If you specify this logo, it replaces the *global* logo in the heading on product pages and request emails for users of the business unit. You can use a business unit logo to support the brand or other messaging uniquely for a business unit. You can update the logos for every business unit or only for specific business units. For example, you can decide to customize logos only for super tenants directly under the root business unit.

If the business unit has child business units, the following applies:

- If the child business unit has its own logo specified, users who log in to it see the child logo, not the parent logo.
- If the child business unit does *not* have its own logo specified, users who log in to it see the global logo.

Thus, users with access to multiple business units can see different header logos when they log in to each business unit.

- The [login page](#) (see page 314) enables a user to access the product.

The same login page (including the login logo) applies to all users in all business units. You can customize the settings for several look-and-feel elements, including images and icons (*except for logos*), menus, tabs, and so forth. When applicable, these elements include colors, font name and point size, highlighting, and related specifications. You customize these look-and-feel elements by editing the Cascading Style Sheet (CSS) files for the login page.

- Global page elements appear on several or all product pages. They include the product name, shopping icon, and footer. Global page elements are always the same, on every product page where they appear.

Like the elements of the login page, global page elements apply to all users, regardless of their business unit. You *cannot* override them with business unit-specific settings. The global page elements also apply regardless of whether you have customized the themes of one or more business units.

You [customize global page elements](#) (see page 328) by editing the file named `includes_shared.xml`.

- A *theme* specifies the settings for several look-and-feel elements, including images and icons (*except for logos*), menus, tabs, and so forth. When applicable, these elements include colors, font name and point size, highlighting, and related specifications. You customize these look-and-feel elements by editing the Cascading Style Sheet (CSS) files for the theme.

The look-and-feel of the UI matches the theme of the business unit that you are logged in to. If theme is not set for a business unit, CA Service Catalog checks the business unit hierarchy until it finds a theme. Thus, if a business unit does not have its own theme, it uses the theme of its closest parent business unit. You can use the same theme for all business units. Alternatively, you can optionally create and use different themes for different business units.

You can customize any, all, or none of the items in this list. Customizing each item in the previous list is a separate, independent operation. You can customize any one of them *without* customizing the others. This separation provides flexibility and efficiently.

You can customize logos or global page elements quickly and easily. Customizing themes is a longer process and requires advanced [prerequisites](#) (see page 323). Verify that the customizations you plan to make to each one are compatible with each other, to help provide a consistent look-and-feel to users.

Upgrade Considerations

The updates in this chapter *replace* any *overlapping* information about custom branding in previous releases, especially concerning the following elements:

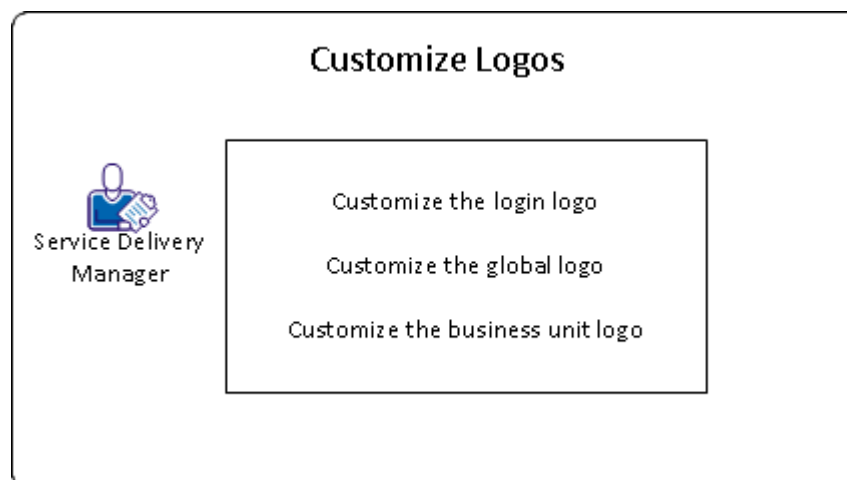
- Logos
- Login page elements
- Global page elements, including icons, footer elements, and header elements

If you customized any of these elements in previous releases, do *one* of the following, whichever applies to your implementation:

- Verify that the customized files reside in a *custom* subfolder of the %USM_HOME%\FileStore folder.
- Otherwise, recreate your customizations by following the instructions in this chapter.

How to Customize Logos

Logos are image files that uniquely identify a company, business unit, or super business unit. As a service delivery manager, you can customize the logos used on the CA Service Catalog UI. Using custom logos helps reinforce branding or other messaging in your organization.



To customize logos on the CA Service Catalog UI, do the following. Each customization is optional.

- [Customize the login logo](#) (see page 311).
- [Customize the global logo](#) (see page 312).
- [Customize the business unit logo](#) (see page 313).

Customize the Login Logo

CA Service Catalog includes a predefined login logo that you can optionally replace with a custom login logo. The login logo *always* applies to the login page, regardless of whether you have specified different logos for different business units. You can use a custom login logo to support the brand or other messaging of your organization.

Follow these steps:

1. Determine the custom login logo that you want to use.
Note: We recommend that you size your custom logo to be approximately the same size as the predefined logo.
2. Access the %USM_HOME%/FileStore/themes/common/images/logo folder on your filestore computer.
3. Copy and rename the predefined login logo (login_logo.png).

4. Copy the custom logo to the same folder. Rename it to the name of the original logo.
5. Access the login page for CA Service Catalog.
6. Verify that the predefined login logo no longer appears and that the custom login logo appears correctly.

You have customized the login logo.

Customize the Global Logo

CA Service Catalog includes a *predefined* global logo that applies to all users. You can optionally replace it with a *custom* global logo to support the brand or other messaging of your organization. The global logo appears in the heading of all product pages (except the login page) and request emails.

Note: If a business unit has its own logo specified, users who log in to it see the business unit logo instead of the global logo.

Follow these steps:

1. Determine the custom global logo that you want to use.
Note: We recommend that you size your custom logo to be approximately the same size as the predefined logo.
2. Access the %USM_HOME%/FileStore/themes/common/images/logo folder on your filestore computer.
3. Copy and rename the predefined global logo (header_logo.png).
4. Copy your custom logo to the same folder. Rename it to the name of the original logo.
5. Log in to CA Service Catalog.
6. Verify that the predefined global logo no longer appears.
7. Verify that your custom global logo is legible on the UI and in request emails, unless a business unit logo overrides it.

You have customized the global logo.

Customize the Business Unit Logo

For each business unit, you can optionally specify a *business unit* logo. If you specify this logo, it replaces the *global* logo in the heading on product pages and request emails for users of the business unit. You can use a business unit logo to support the brand or other messaging uniquely for a business unit. You can update the logos for every business unit or only for specific business units. For example, you can decide to customize logos only for super tenants directly under the root business unit.

Important! If you have enabled multi-tenancy with CA Service Desk Manager, CA Service Catalog ignores any of its own settings for business logos. Instead, CA Service Catalog uses the logo or logos that the CA Service Desk Manager setup specifies, if applicable. If no CA Service Desk Manager logo applies, then each business unit uses the CA Service Catalog global logo.

Follow these steps:

1. Determine the business unit logo that you want to use.
Note: We recommend that you size your logo to be approximately the same size as the predefined global logo.
2. (Optional) Do the following:
 - Rename the custom logo file intuitively to match its business unit. For example, for a business unit named Vienna_123, name the logo Vienna_123_header_logo.png.
 - Create a subfolder named "custom logos" or something similar under %USM_HOME%/FileStore/themes/common/images/logo.
3. Copy your custom logo to the %USM_HOME%/FileStore/themes/common/images/logo folder on your filestore computer.
4. In CA Service Catalog, do *one* of the following, whichever applies to your level of administrative access:
 - Log in to the business unit whose logo you want to change.
 - Log in to the root business unit and do the following:
 - a. Select Administration, Business Units.
 - b. Drill down the tree to the business unit whose logo you want to change.
5. Edit the business unit.
6. In the Logo field, enter the URL of the logo that you copied and save your changes.
7. Refresh your browser.

8. Verify that your business unit logo is legible on the UI and in request emails.
9. If the business unit has child business units, verify the following:
 - If the child business unit has its own logo specified, users who log in to it see the child logo, not the parent logo.
 - If the child business unit does *not* have its own logo specified, users who log in to it see the global logo.

Thus, users with access to multiple business units can see different header logos when they log in to each business unit.

You have specified a business unit logo.

Customization of the Login Page

CA Service Catalog includes a predefined login page that you can optionally customize, to reinforce branding or other messaging. The same login page applies to all users, regardless of the business unit that they are logging in to.

You can customize the login page, as follows:

- [Customize the login logo](#) (see page 311).
- Customize the *look-and-feel* of several elements of the login page by [editing the logon.css file](#) (see page 316).
 - Before you edit the logon.css file, verify that you meet the [prerequisites for editing CSS files](#) (see page 323).
- Customize the *content* or *text* of the [elements on the login page](#) (see page 318).

Keep in mind the following important points:

- You can customize the login page *without* customizing the [theme](#) (see page 320) for one or more business units. The same login page applies to all users, regardless of whether you have customized any theme.

Customizing the login page includes some of the same steps as customizing a theme. However, the two customizations are separate and independent of each other. This separation provides greater flexibility to your organization. This separation also enables you to update the login page alone more quickly and more efficiently.

- Review the [overview of custom branding](#) (see page 309) for important information about logos, the login page, themes, and global page elements. Verify that the customizations you plan to make to each one are compatible with each other, to help provide a consistent look-and-feel to users. For example, using similar colors and elements on both the login page and the product pages helps provide a consistent user experience.

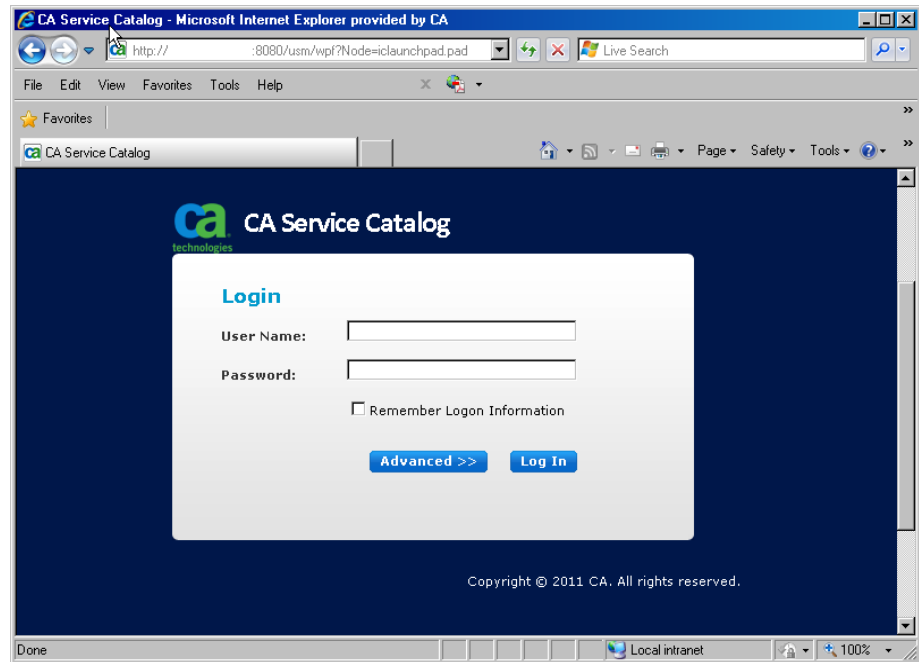
Customize the Login Page

As part of customizing your implementation, you can [customize](#) (see page 314) the look-and-feel of the login page to reinforce branding or other messaging. The same login page applies to all users, regardless of business unit that they are logging in to. Before you edit the logon.css file, verify that you meet the [prerequisites for editing CSS files](#) (see page 323).

Follow these steps:

1. Open your web browser and access the login page for CA Service Catalog.

For example, for the predefined CA_Technologies_r7 theme, before you make any customizations, the login page appears similar to the following:



2. Back up the %USM_HOME%\filestore\themes\common\css\logon.css file.

Important! As a best practice, *always* back up CSS files and other configuration files before editing them.

3. Open the file, using the CSS editor for your web browser.
4. Find the lines that control the look-and-feel specification that you want to update.

For example, to configure the look-and-feel of the product name, find the following line:

```
.loginproductname {  
    text-align: left;  
    font-family: CAlibri, Verdana, Arial, Helvetica, sans-serif;  
    color: #ffffff;  
    ...  
}
```

5. Update the lines to match the look-and-feel specification you want, and save the file.

For example, for the previous step, to change the color of the product name from the current color to blue, update the lines as follows:

```
.loginproductname {  
  text-align: left;  
  font-family: Calibri, Verdana, Arial, Helvetica, sans-serif;  
  color: blue;  
  ...  
}
```

6. Repeat the previous step for other look-and-feel changes that you want to make.

For example, to configure the background color of the login page, find the following lines:

```
.login_page {  
  background-color: #00174A;  
  text-align: center;  
  ...  
}
```

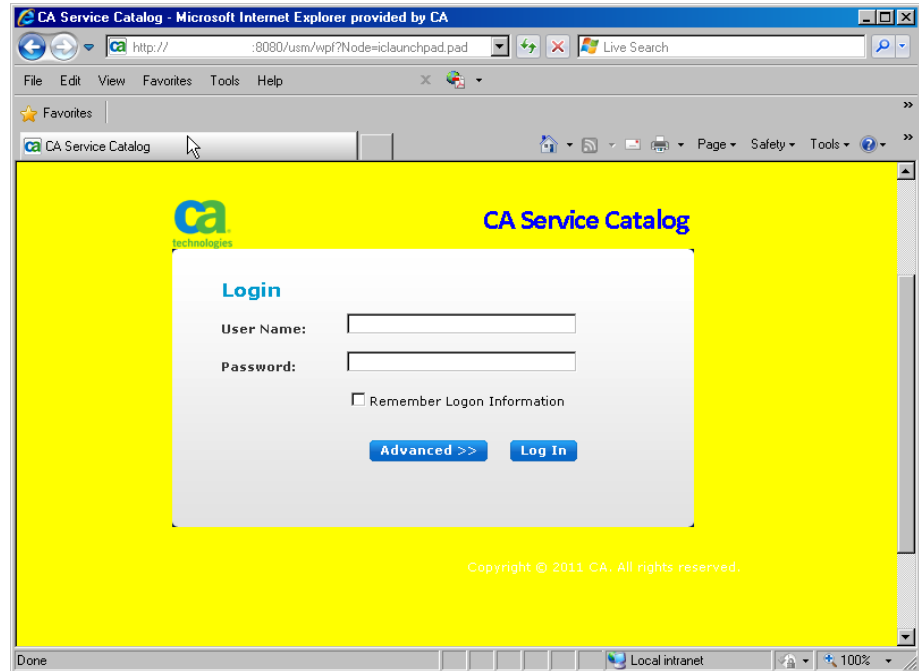
7. Update the lines to match the look-and-feel specification you want, and save the file.

For example, consider the previous step. To change the background color of the login page to yellow and align the affected text to the right, update the lines as follows:

```
.login_page {  
  background-color: yellow;  
  text-align: right;  
  ...  
}
```

- Refresh your browser and verify your updates on the login page.

For example, the following page reflects the customizations made in the previous steps. The product name is blue. The background color is yellow. The affected text is aligned on the right.



- Update the [elements of the login page](#) (see page 318) to meet your requirements. Verify each change by saving the file and refreshing the login page.

You have customized the login page.

Elements on the Login Page

The following table lists the elements of the login page that you are most likely to customize, except for the [login logo](#) (see page 311). When applicable, each row lists the section of the login.css file that affects the look-and-feel of the element. Callout numbers identify these elements in the sample page that appears after the table.

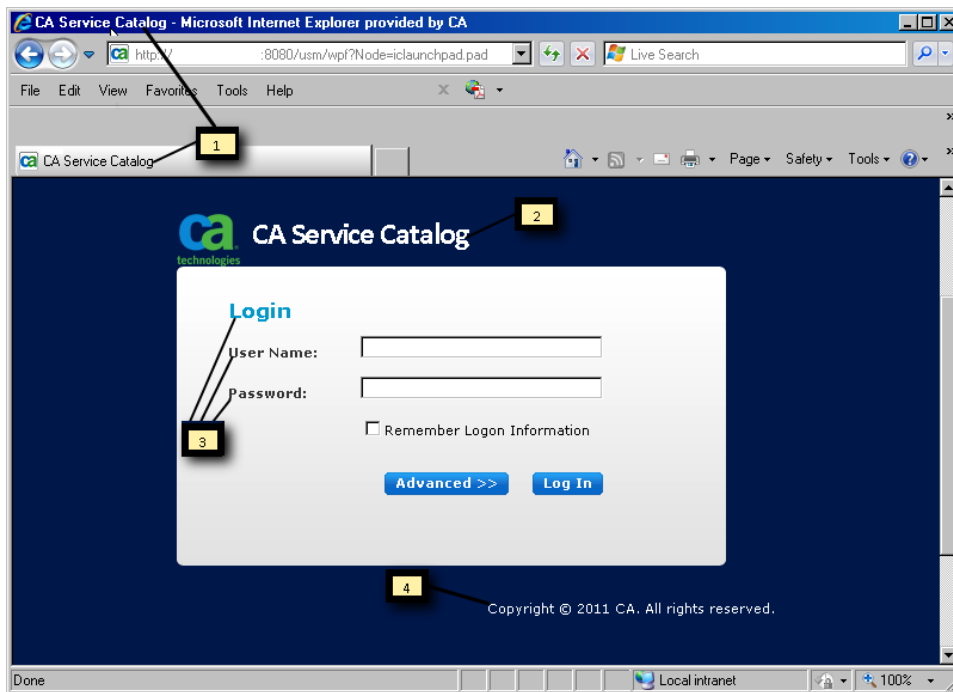
Callout Number	GUI Element	File Location under %USM_HOME%/	Section in Logon.css File
1	Text for browser window title and title bar	view\webapps\usm\locale\icusen\logon.xml	.loginpage
2	Text for product name	view\webapps\usm\locale\icusen\logon.xml	.loginproductname

3	Login input text	view\webapps\usm\locale\icusen\logininputtextgon.xml	logininputtext
		Note: This text supplies the User Name, Password, and Advanced-Business Unit fields.	
4	Copyright text and date	view\webapps\usm\locale\icusen\loginpagecopyrightgon.xml	.loginpagecopyright

In addition, the favorites icon appears in the browser address bar and the product title bar of every product page, including the login page. The favorites icon is a [global page element that you can customize](#) (see page 328).

Note: For the Text elements, the File Name column displays the folder location for an English system (icusen). For other languages, the location is different.

Each element in the following picture matches a callout item from the preceding table. You can optionally customize the item by replacing or editing the corresponding file. Your browser page can look different from the following example.



Themes

A *theme* specifies the settings for the following look-and-feel elements:

- Images and icons (*except for logos*)
- Menus
- Tabs
- Toolbars
- Wizards

When applicable, these elements include the following specifications:

- Colors (especially background colors)
- Font name and point size
- Highlighting, such as bold or underline
- Position on a page or dialog

You customize these look-and-feel elements by editing the Cascading Style Sheet (CSS) files for the theme. Each theme includes the following CSS files:

- `logon.css`, which applies to the login page *only*
- `main.css`, which applies to other product pages

Important! *Always back up a CSS file before editing it, so that you can return to the original specifications if necessary.*

You copy and modify predefined CSS files as part of the process of [creating a theme](#) (see page 324).

A theme is [organized](#) (see page 321) in folders, with one top-level folder for each theme. In addition to the CSS files, a theme includes several other supporting files and several folders. You do not need to edit these additional files and folders. However, you copy them as a group when you copy and modify a CSS file.

Review the [overview of custom branding](#) (see page 309) for important information about logos, the [login page](#) (see page 314), themes, and [global page elements](#) (see page 327). Verify that the customizations you plan to make to each one are compatible with each other, to help provide a consistent look-and-feel to users.

Predefined and Custom Themes

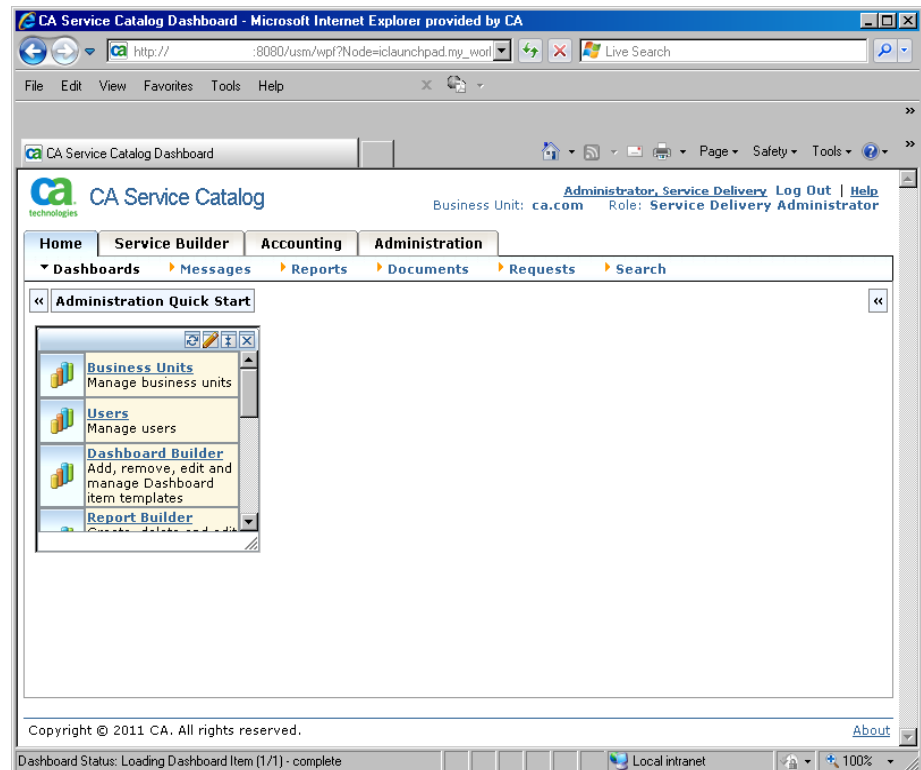
A theme is organized in folders, with one top-level folder for each theme. In addition to the CSS files, a theme includes several other supporting files and several folders. You do not need to edit these additional files and folders. However, you copy them as a group when you copy and modify a CSS file.

In the %USM_HOME%\filestore\themes folder, CA Service Catalog includes the following top-level folders for each predefined theme:

- CA_Technologies_R5

Specifies the predefined look-and-feel elements of *previous* releases of CA Service Catalog.

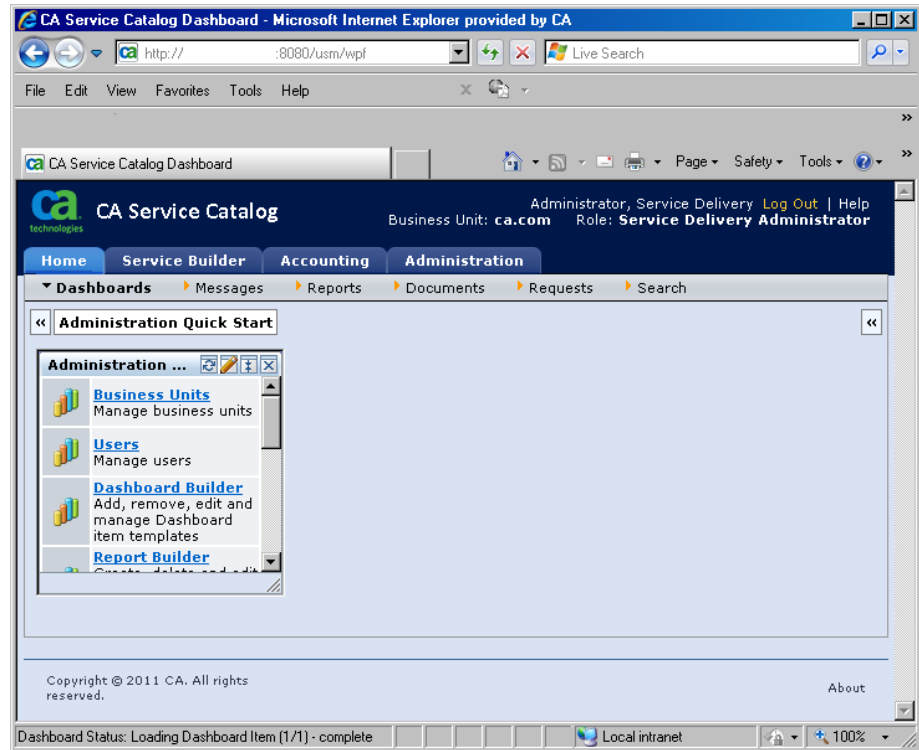
The following is a sample home page using this theme (without customizations):



- CA_Technologies_R7

Specifies the predefined look-and-feel elements of the *current* release of CA Service Catalog.

The following is a sample home page using this theme (without customizations):



- common

Contains look-and-feel elements that apply to *all* predefined and custom themes.

Important! Do *not* copy and modify the *common* folder.

If you have already created custom themes, your top-level folders for those themes also appear in the %USM_HOME%\filestore\themes folder.

To create a custom theme, you copy either a predefined folder (such as CA_Technologies_R7) or a custom folder that you created earlier. Afterwards, you modify the CSS file of interest in the folder that you copied.

You store all custom theme folders under the filestore folder. You store them on the same folder level as the CA_Technologies_R5 and CA_Technologies_R7 folders.

Each top-level folder name becomes the name of an option for a theme. When you edit a business unit, you can select a theme for it.

If you update a theme for a specific business unit, the change affects the users who belong to that business unit. The change also affects any child business units that do not have their own theme specified. Child business units inherit the theme of their parent business unit. However, they can optionally override the inherited theme by specifying their own theme.

Customization of Themes

The look-and-feel of the UI matches the theme of the business unit that you are logged in to. If theme is not set for a business unit, CA Service Catalog checks the business unit hierarchy until it finds a theme. Thus, if a business unit does not have its own theme, it uses the theme of its closest parent business unit. You can use the same theme for all business units. Alternatively, you can optionally create and use different themes for different business units.

To customize a theme, you do the following:

- [Create](#) (see page 324) a custom theme for one or several business units.
- [Customize](#) (see page 325) the theme you created by editing its main.css file.

Before you edit the main.css file, verify that you meet the [prerequisites for editing CSS files](#) (see page 323).

Prerequisites for Editing Themes

As an administrator, edit the theme for one or more business units *only* if you have expertise in the following areas:

- UI design, especially look-and-feel elements
- Standard specifications for CSS files
- Customization of CSS files, using a CSS file editor for your web browser

How to Create Custom Themes

You create a custom [theme](#) (see page 320) by copying and modifying an existing theme. You can copy and modify either a predefined CA Service Catalog theme or another existing theme that you created earlier. Using a custom theme for a business unit helps support branding or other messaging for the business unit and, optionally, its child business units.

Important! As a best practice, do *not* modify a predefined CA Service Catalog theme directly. Instead, copy and modify it, so that you can efficiently return to the original version, if necessary. *Always* back up CSS files before editing them.

To customize a theme, follow this process:

1. Verify that you meet the [prerequisites for editing themes](#) (see page 323).
2. Access the computer on which the filestore resides.
3. Find and expand the %USM_HOME% folders. Expand the \filestore\themes folder. Review the organization of the [predefined and custom themes](#) (see page 321) in that folder.

Note: The name of each top-level folder is the name of an option that you can select when you select a theme for a business unit.

4. Copy the top-level folder of existing theme that you want to use as a starting point for your new theme.
5. Wait for the copy operation to finish and rename the new theme.

For example, suppose the existing theme was named Rome_Super_Tenant_A. If the new theme is for a second super tenant, you can name it Rome_Super_Tenant_B. Conversely, if the new theme is for a new child business unit of the parent super tenant, you can name it Rome_Super_Tenant_A--Child-1.

6. Add or edit the business unit for which you want to use this theme. In the Available Branding field, select the new theme that you created.

For example:

- To apply the theme to all business units that do not have their own theme, edit the root business unit and apply this theme.
- To apply the theme to a specific business unit, add or edit the business unit and apply the theme.

The theme also applies to all child business units that do not have their own theme.

7. [Customize the new theme](#) (see page 325) by editing its main.css file.

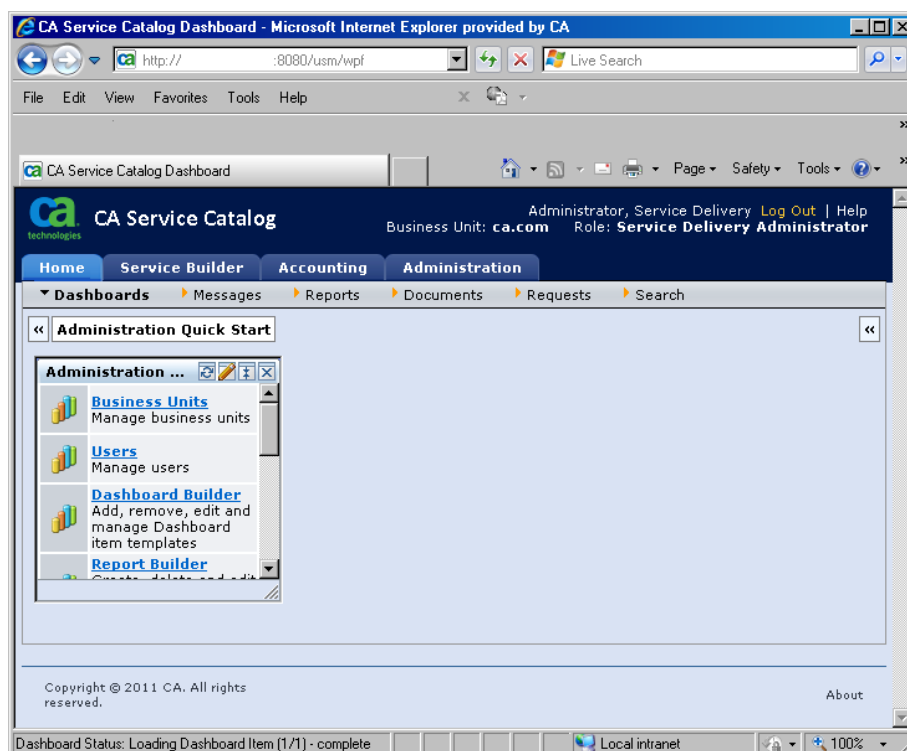
You have created the new theme and are now ready to begin customizing it.

Customize a Theme

After you have created a theme, you can customize it, to give it a unique look-and-feel. Customizing a theme helps to reinforce branding and other messaging for the business unit or the department or organization it represents. Before you edit the main.css file, verify that you meet the [prerequisites for editing CSS files](#) (see page 323).

Follow these steps:

1. Log in to CA Service Catalog and note the look-and-feel of the home page. The following sample home page uses the default settings of the CA_Technologies_R7 theme:



2. Back up the main.css file in the [custom theme folder that you created](#) (see page 324). A sample path name is %USM_HOME%\filestore\themes\custom_theme\css\main.css file.

Important! As a best practice, *always* back up CSS files and other configuration files before you edit them.

3. Open the main.css file of your custom theme. Use a suitable CSS editor for your web browser.

- Find the lines that control the look-and-feel specification that you want to update.

For example, To change the background color globally on product pages, do the following:

- Find the following default setting:

```
td.pagebg{background-image:url(../images/grid/page-bg.png);background-repeat:repeat-x;background-color:#D9E2F3;}
```

- Delete the following phrase:

```
background-image:url(../images/grid/page-bg.png);
```

The line now appears as follows:

```
td.pagebg{background-repeat:repeat-x;background-color:#D9E2F3;}
```

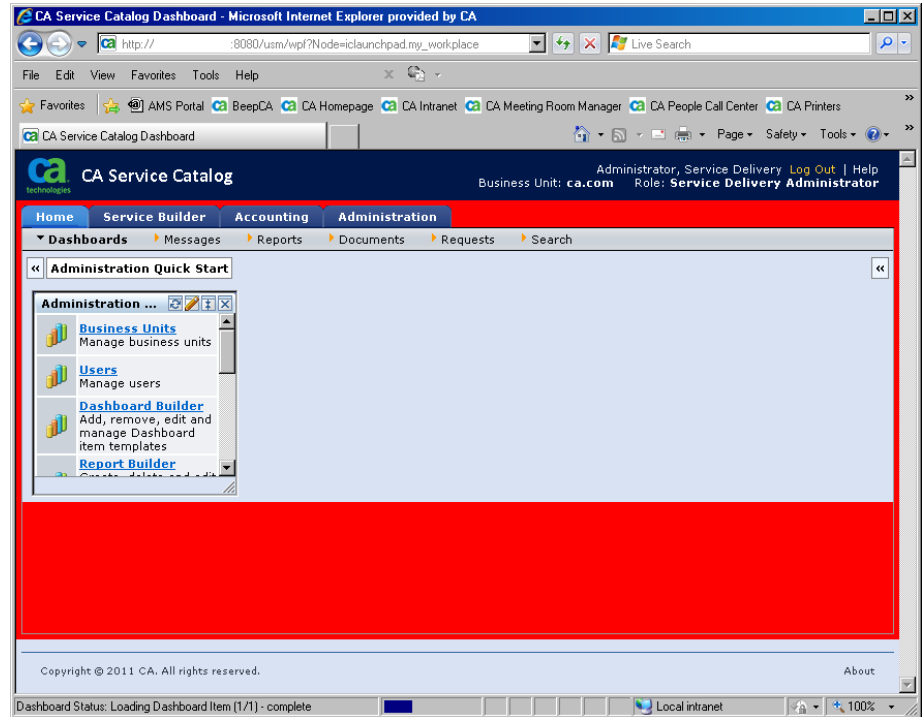
- Change the background-color:#D9E2F3 to the color of your choice, for example, background-color:red.

- Save the file.

Note: The setting in this example *does* affect the background color of the *entire* product page. However, the background colors of specific sections of the page *override* the background color of the entire page.

- Refresh the CA Service Catalog UI. Verify the changes to the product pages.

A sample page follows. This page displays the updates to the background color specified in the previous step.



6. Update other elements of the theme meet your requirements. Verify each change by saving the file and refreshing the login page.

For example, you can customize the look-and-feel of the top-level menu tabs (Home, Service Builder, Accounting, and Administration). To do so, find and edit the following section in the main.css file:

```
a.tabs {
font-family:verdana, arial,sans-serif;
font-size:10px;
font-weight:700;
color:yellow;
text-align:center;
white-space:nowrap;
text-decoration:none;}
```

7. If necessary, refine your original edits of the main.css file, or create additional customizations. Verify your updates on the UI, as explained in the previous steps.

You have customized the theme. In addition, you can also customize certain [global page elements](#) (see page 327) that are not directly related to themes.

Global Page Elements

You can customize certain global page elements. Like the elements of the login page, global page elements apply to all users, regardless of their business unit. The global page elements also apply regardless of whether you have customized the themes of one or more business units.

Global page elements appear on several or all product pages. They include the product name, shopping icon, and footer.

You [customize global page elements](#) (see page 328) by editing the file named includes_shared.xml.

Review the [overview of custom branding](#) (see page 309) for important information about logos, the login page, themes, and global page elements. Verify that the customizations you plan to make to each one are compatible with each other, to help provide a consistent look-and-feel to users.

Customize Global Page Elements

As part of customizing your implementation, you can customize global page elements to reinforce branding or other messaging. These elements include both text and icons. The same global page elements apply to all users, regardless of business unit that they are logging in to.

Follow these steps:

1. Back up the %USM_HOME%\view\webapps\usm\locale\icusen\includes_shared.xml.

Important! As a best practice, always back up XML files and other configuration files before editing them.

2. Open the includes_shared.xml file, using the XML editor of your choice, for example, Windows Notepad.

Note: The folder location is for an English system (icusen). For other languages, the location is different.

3. Find the line that controls the text that you want to update. Some sample settings follow:

- Text for the product name: <product_title> value
Default: CA Service Catalog
- Text for the Logout button: <logoutnode> value
Default: Log Out
- Text for the footer: <footer> value
Default: Copyright (c) 2011. All rights reserved.

4. Update the lines to the values you want, and save the file.
5. Access the folder that contains the icons that you want to update.

Sample icons and their file names follow, according to the folder in which they reside:

- %USM_HOME%\view\webapps\usm\images folder:
 - Add: tb_add.png
 - Calendar: calendar.gif
 - Edit: edit.gif
 - Refresh: reset.gif
 - Search: icon-search.gif
 - Shopping cart: shopping_cart.png

- %USM_HOME%\view\webapps\root folder:
 - favicon.ico

The favorites icon appears in the browser address bar and the product title bar of every product page, including the [login page](#) (see page 318).

Note: To view an icon, double-click its file name.

6. Do the following for each icon that you want to change:
 - a. Rename the original file to filename_OLD.png.
 - b. Copy your new file to the folder, and rename it to the original file name.

For example, first rename the original shopping_cart.png to shopping_cart_OLD.png. Next, copy your new shopping cart icon to the folder and rename it to shopping_cart.png.

7. Log in to CA Service Catalog and verify your updates on the product UI. For completeness, review several pages of the UI.
8. Repeat the previous steps, if necessary, until the UI matches your specifications.
9. Copy the icons that you customized to the %USM_HOME%\filestore\custom\images folder.

Important! This step is required to help ensure that your updates apply to all users in your organization.

You have customized the global page elements.

Customize the Online Help

Service delivery administrators can optionally replace the predefined online help with custom online help, for any, some, or all roles. Here, the predefined online help refers to the *Administration Guide* and the other guides that are linked to it. The custom online help appears instead of the predefined online help when users with the specified roles click the Help button on the top right of any page.

Note: If the user selects Administration, Tools, Links, Documentation, the predefined online help *always* appears. This menu selection is *not* affected by the customization in this topic for the online help that appears when users click the Help button.

Follow these steps:

1. Create your custom online help file files and copy them to the %USM_HOME%\filestore\custom\help\language folder.

language

Specifies the language of the operating system on which you installed CA Service Catalog. For example, specify en_US for U.S. English or ja_JP for Japanese.

Note: The folder must include an index.html file that, when clicked, opens the custom online help.

2. Click Administration, Configuration, Filestore.
3. Select the option named Enable Custom Help.
4. Specify the roles that you want to see the custom help rather than the predefined online help.
5. Restart Service View.
6. Verify that CA Service Catalog functions as expected when users with the specified roles click the Help button on the top right of any page:
 - If applicable, the custom online help opens instead of the predefined online help.
 - If the index.html file does *not* exist in the %USM_HOME%\filestore\custom\help\language folder, the index.html file in the %USM_HOME%\filestore\custom\help/default folder runs.
 - If no previous bullet applies or if the custom online help is disabled, the predefined online help opens.

Chapter 13: Uninstalling

This section contains the following topics:

[How to Uninstall CA Service Catalog](#) (see page 331)

[Uninstall CA Service Catalog Components](#) (see page 332)

How to Uninstall CA Service Catalog

You can uninstall the products and components of CA Service Catalog. Uninstall each product or component, as follows:

1. Stop all CA Service Catalog services on all CA Service Catalog computers.

The CA Service Catalog services are named Message Queue 4.1 Broker, Service View, CA Service Accounting, and CA Service Fulfillment.

2. [Uninstall](#) (see page 332) CA Service Accounting, CA Workflow, and Service View on distributed computers, if applicable.

Distributed computers are computers *other than the first (formerly primary) Service View* computer.

3. [Uninstall](#) (see page 332) CA Workflow, CA Service Accounting, and Catalog content on the first Service View computer, if applicable.
4. [Uninstall](#) (see page 332) CA Service Catalog on the first Service View computer.
5. [Uninstall](#) (see page 332) the first Service View computer.

During this time, you are prompted to either keep or delete the CA Service Catalog data in the MDB.

As a best practice, keep the data for backup purposes or for use by any future installations of CA Service Catalog in your enterprise.

Note: If you delete the data, it cannot be recovered.

6. [Uninstall](#) (see page 332) CA EEM if it not used by other CA products.

Note: Tomcat and the JRE are installed automatically during the CA Service Catalog installation. They are left installed so that other components and products can use them.

Uninstall CA Service Catalog Components

You can use the installation program to uninstall each CA Service Catalog component.

To uninstall CA Service Catalog components

1. Access the installation media and run setup.exe.
The installation Product Explorer window appears.
2. Select the product or component and click Uninstall.
3. Follow the prompts as the installation wizard guides you through the process to uninstall the component.

You have uninstalled CA Service Catalog components.

Appendix A: Troubleshooting

This section contains the following topics:

- [Scope](#) (see page 333)
- [Cannot Log In to CA Service Catalog](#) (see page 334)
- [Cannot Add or Update a User Because of Duplicate User ID](#) (see page 335)
- [Cannot Delete an Account](#) (see page 336)
- [Cannot Connect to a Trusted Computer](#) (see page 336)
- [Cannot Email a Request](#) (see page 337)
- [Cannot Locate the Configuration Files](#) (see page 337)
- [Cannot Locate My Log Files](#) (see page 338)
- [Compilation Errors After Customization](#) (see page 338)
- [Log File Does Not Roll Over](#) (see page 338)
- [Cannot Locate the Registry Keys](#) (see page 339)
- [Cannot Set Debug Levels](#) (see page 340)
- [Cannot Open Documents from the Web Folder](#) (see page 340)
- [Message Queue 4.1 Broker Stops Immediately After Starting](#) (see page 340)
- [Message Queue 4.1 Broker Does Not Respond to Scans](#) (see page 341)
- [In HTTPS, Unable to View Invoice in CSV Format from Invoice History UI](#) (see page 342)
- [IXUTIL Out-of-Memory Error Occurs](#) (see page 343)
- [Pages Do Not Appear to Be Refreshing Properly](#) (see page 343)
- [A Request Approval or Fulfillment Pending Action Is Not Assigned](#) (see page 343)
- [Requests Are Assigned to Multiple Users and Groups](#) (see page 344)
- [Requests Do Not Move to the Next Status](#) (see page 345)
- [Sorting of Services by Selection Type](#) (see page 347)
- [Service View Installation or Upgrade Fails Because Path Name is Too Long](#) (see page 347)
- [Service View Installation or Upgrade Fails Because of Duplicate Records](#) (see page 348)
- [Service View Windows Service Does Not Start](#) (see page 348)
- [CA EEM Installation on 64-Bit Operating Systems](#) (see page 349)
- [CA EEM Upgrade Fails](#) (see page 349)

Scope

This appendix contains *only* troubleshooting topics related to the core components of the product: CA Service Catalog, CA Service Accounting, Service View, and Service Fulfillment.

Note: For additional troubleshooting topics related to the integration of CA Service Catalog with other products, including CA Workflow, CA EEM, CA Service Desk Manager, and so on, see the *Integration Guide*.

Cannot Log In to CA Service Catalog

Symptom:

I cannot log in to a CA Service Catalog computer.

Solution:

Try the following:

- Verify that your user name and password are valid.
- Verify that CA Service Catalog services are running on the computer that you are trying to log in to.
- Verify that *no* underscore character (_) appears in the CA Service Catalog computer name, if you are using Microsoft Internet Explorer to access CA Service Catalog. If an underscore appears in the computer name, do one of the following:
 - Use Mozilla Firefox or Safari instead of Internet Explorer to access CA Service Catalog.
 - Rename the computer to remove the underscore, and update all references to the computer name throughout your environment. Then continue to use Internet Explorer to access CA Service Catalog.

For more information about this issue in Internet Explorer, see the related information in the knowledge base (KB) on the Microsoft website, microsoft.com. At publication time, the most relevant KB article is 325192, "Issues after you install updates to Internet Explorer or Windows."

Cannot Add or Update a User Because of Duplicate User ID

Symptom:

When I try to add a new user or update an existing user ID, I receive an error message like the following:

Error - User with this user id already exists. Choose a different user id.

Solution:

A duplicate user profile exists. This problem can occur even if that user has been deleted. Deleted users are marked as inactive but are retained in the database.

Before assigning the user ID to a different user, remove the user ID from the inactive user.

To remove a user ID from an inactive user

1. Click Administration, Users.
The Search User options appear.
2. Click the View Advanced icon option of the Search Users options.
The Advanced Search fields appear.
3. Select User ID from the list of fields and select Contains from the list of operators.
4. Enter the user ID in the value field and click the Add link.
5. Select Inactive from the list of fields and select Equals from the list of operators.
6. Enter 1 for "true" in the value field and click the Add link.
7. Click Search.
The list of users that match the selection criteria appears.
8. Edit the user: Change, or clear the User ID field, and click OK.

Cannot Delete an Account

Symptom:

When I try to delete an account, a message appears indicating that I cannot delete this account.

Solution:

You cannot delete an account with an active subscription.

Before you delete an account, prepare to delete it.

To prepare to delete an account

1. Cancel the subscriptions associated with the account.
2. Close the account by setting the status of the account to Closed.
3. Verify that all the billing runs affecting the account are completed.

Note: For details about performing these tasks, see the *Administration Guide*.

Cannot Connect to a Trusted Computer

Symptom:

I have configured CA Service Catalog and an integrating product, such as CA Service Desk Manager, to use Secure Socket Layer (SSL) to connect to each other using a trusted relationship. However, when I test the connection, it fails, and I receive error messages that no trusted relationship exists.

Solution:

- Verify that you have [configured CA Service Catalog to use SSL](#) (see page 106).
- Verify especially that you have [added self-signed certificates to the keystore](#) (see page 116), if applicable

When you use *self-signed* certificates for any computer that connects directly to CA Service Catalog or that CA Service Catalog connects to, add these certificates to the keystore. For example, suppose you are using [clustering](#) (see page 215) with [load balancing](#) (see page 236) for CA Service Catalog. In that case, if you are using a self-signed certificate for the load balancing computer, add them the keystore.

Moreover, verify the computer to be trusted, that is, the computer that has direct connection with CA Service Catalog. For example, suppose you integrate CA Service Catalog with CA Service Desk Manager through a load balancing computer. In that case, CA Service Catalog connects directly to the load balancer (not CA Service Desk Manager). Therefore, the computer to be trusted is the load balancer (not the CA Service Desk Manager computer).

Cannot Email a Request

Symptom:

I have CA EEM configured to use an external directory containing many groups. When emailing a request, I get the error "Cannot send email, please contact your administrator."

Solution:

Increase the value of the CA EEM Max Search Size to process the number of groups defined in your external directory.

To set the CA EEM Max Search Size

1. Start the CA EEM user interface by clicking the Administration Quick Start menu Embedded CA EEM link.
The CA EEM login screen appears.
2. Log in using the EiamAdmin user name and password.
The CA EEM Home Page appears.
3. Click the Configure, Session, Configuration menu option.
The Session Configuration screen appears.
4. Change the Max Search Size to a value larger than the number of groups in your external directory.
5. Click Save.

Cannot Locate the Configuration Files

Symptom:

I cannot locate my CA Service Catalog configuration files.

Solution:

The configuration files and locations are as follows:

- Database connection configuration file: %USM_HOME%\DBSource.properties
- CA EEM connectivity configuration file: %USM_HOME%\Eiam.properties
- Ixutil utility configuration file: %USM_HOME%\scripts\ixutil.cfg

Cannot Locate My Log Files

Symptom:

I cannot locate my CA Service Catalog log files.

Solution:

See the [names and locations of all log files](#) (see page 205).

Compilation Errors After Customization

Symptom:

After I customized files, I began receiving multiple compilation-related error messages in the log files of additional Service View computers. These error messages appear similar to the following:

...

```
yyyy/mm/dd computer-name-or-address ERROR [TP-Processor21] [DomProcessor] Error Generating Document  
javax.xml.transform.TransformerConfigurationException: Could not compile stylesheet
```

...

Solution:

Do the following:

- Review the instructions for [customizing XSL, XML, JavaScript, and image files](#) (see page 306). Verify that you have followed all instructions.
- Verify that the [filestore](#) (see page 187) is set up correctly. Especially verify that *all* Service View computers share the filestore.

Log File Does Not Roll Over

Symptom:

The log file does not roll over: The log file is not automatically renamed and started over again when it reaches a specific maximum size. Instead, the log file grows continuously without limit until I manually delete or rename it.

Solution:

Review and follow the process for [configuring rollover settings for selected log files](#) (see page 213).

Cannot Locate the Registry Keys

Symptom:

I cannot locate my CA Service Catalog registry keys.

Solution:

The following are the CA Service Catalog registry key locations for 32-bit operating systems:

- Service View
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Service Catalog\View
- CA Service Catalog
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Service Catalog\Catalog
- CA Service Catalog Content
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Service Catalog\Catalog Content
- CA Service Accounting
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Service Catalog\Accounting
- CA Workflow
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Service Catalog\Fulfillment

The following are the CA Service Catalog registry key locations for 64-bit operating systems:

- Service View
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\Service Catalog\View
- CA Service Catalog
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\Service Catalog\Catalog
- CA Service Catalog Content
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\Service Catalog\Catalog Content
- CA Service Accounting
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\Service Catalog\Accounting
- CA Workflow

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\Service Catalog\Fulfillment

Cannot Set Debug Levels

Symptom:

I do not know how to set my debug levels.

Solution:

Follow the process for [setting log levels](#) (see page 210).

Cannot Open Documents from the Web Folder

Symptom:

This issue applies *only* if you are using Office 2007.

In CA Service Catalog, I attempted to open a text file or PDF file by clicking Home, Documents, View Content, Open as Web Folder. When I clicked the file that I wanted, I was not able to open it.

Solution:

1. Locate the Microsoft Office 2007 post-Service Pack 1 hotfix 943337 on the Microsoft website, microsoft.com.
2. Follow the instructions from Microsoft to download and apply the hotfix locally on the computer from which you access CA Service Catalog.
3. Reboot the computer.
4. Log in to CA Service Catalog.
5. Click Home, Documents, View Content, Open as Web Folder.
6. Verify that you can access both text and PDF files.

Message Queue 4.1 Broker Stops Immediately After Starting

Symptom:

At times, Message Queue 4.1 Broker stops immediately after starting.

Solution:

Before you start Message Queue 4.1 Broker, delete the file named “lock” in the folder named CA\Service Delivery\view\conf\var\instances\imqbroker.

Message Queue 4.1 Broker Does Not Respond to Scans

Symptom:

In some cases, Message Queue 4.1 Broker fails to respond when I scan the computer on which it is installed for security or port data.

Solution:

The cause could be that Message Queue 4.1 Broker is using dynamic ports (its default setting).

To help enable Message Queue 4.1 Broker to repond to scans, configure it to bind to static ports and IP addresses.

To Configure Message Queue 4.1 Broker to bind to static ports and IP addresses

1. Using the Windows Control Panel, stop the Windows service named MessageQueue 4.1 Broker.
2. Open the Message Queue 4.1 Broker configuration file named default.properties for editing.

The default location of this file is C:\Program Files\CA\SC\MessageQueue\4.1\mq\lib\props\broker.

3. Search for the following string and change the current value (likely 0) to 2202:
imq.jms.tcp.port=

4. Search for the following string:
imq.jms.tcp.hostname=

Do the following, if they are not already done:

- Delete the pound sign (#) from the beginning of this string
- Specify the host name of the computer on which the Message Queue 4.1 Broker is installed

5. Search for the following string and change the current value (likely 0) to 2203:
imq.admin.tcp.port=

6. Search for the following string:
imq.admin.threadpool_model=dedicated

Add a new line underneath it and enter the following string:

imq.admin.tcp.hostname=127.0.0.1

Note: This value (127.0.0.1) specifies the loopback address, which is accessible only by the computer on which the Message Queue 4.1 Broker is installed.

7. Search for the following string:
imq.portmapper.hostname=
Do the following, if they are not already done:
 - Delete the pound sign (#) from the beginning of this string
 - Specify the host name of the computer on which the Message Queue 4.1 Broker is installed
8. Save the file.
9. Start the MessageQueue 4.1 Broker service.

You have configured Message Queue 4.1 Broker to respond to port and security scans.

In HTTPS, Unable to View Invoice in CSV Format from Invoice History UI

Symptom:

I am using Internet Explorer to access CA Service Catalog. When I try to view invoices in CSV format from Invoice History in an HTTPS environment, the invoices do not display correctly.

Solution:

Update your Internet Explorer settings to display these invoices correctly.

To update Internet Explorer settings to display invoices in CSV format

1. Open the Internet Explorer browser.
2. Select Tools, Internet Options, Advanced tab.
3. Scroll down to the Security setting.
4. Select the checkbox named Do not save encrypted pages to disk.
5. Click Apply.
6. Verify that the invoices display correctly.

IXUTIL Out-of-Memory Error Occurs

Symptom:

When I try to use the IXUTIL utility to import or export CA Service Catalog data, the attempt fails. I receive an error message, such as a "generic" SAXException error.

Solution:

Use a text editor to open the ixutil.bat file and increase the size of the JVM parameter in the ixutil.bat file to 1024 or higher. This setting refers to kilobytes (KB). The ixutil.bat file is located in the %USM_HOME%\scripts folder.

Pages Do Not Appear to Be Refreshing Properly

Symptom:

When I access CA Service Catalog, the pages do not appear as expected in my web browser.

Solution:

Set your browser cache settings to retrieve an updated page from the server on every visit to the page.

Note: For instructions, see the documentation for your web browser.

A Request Approval or Fulfillment Pending Action Is Not Assigned

Symptom:

An approval or fulfillment task for a request is assigned to a user or group. However, the request does not appear in the pending action list for the user.

Solution:

User ID or group names longer than 50 characters are not supported.

Requests Are Assigned to Multiple Users and Groups

Symptom:

CA Service Catalog assigns requests pending action to multiple users and groups.

Solution:

If both the following conditions exist, CA Service Catalog assigns requests pending action to *both* an Application group and a Global group that are defined in CA EEM:

- Both groups have the same name in CA EEM
- Both groups are configured to approve requests

Consider renaming one of the groups or configuring one of them *not* to approve requests.

Requests Do Not Move to the Next Status

Symptom:

Requests do not move to the next status of the request lifecycle as expected, for example, from Submitted to Pending Approval.

Solution:

To move requests to the next status of the request lifecycle as expected, verify the related date settings.

To move requests to the next status of the request lifecycle

1. Identify the status change where requests are getting stuck; for example, the Approved status.
2. Verify that the related CA Process Automation processes or CA Workflow process definitions are activate.
3. Complete this step if you are using CA Workflow; otherwise, skip this step:

Verify that the active dates for the CA Workflow process definitions match the date specified on the computer on which they are installed.

For example, suppose that on May 10, you create a process definition for approving requests and specify it to activate the next day, May 11. However, the date setting on the computer where the process is installed is May 8, two days earlier than the actual date. In this case, your new process definitions is not activated until the computer date setting reaches May 10, even though the actual date is May 12. Consequently, requests do not start being approved again until then. To correct this problem and activate the process definitions immediately, verify that the computer date setting and activation date of the process are the same.

Note: For help setting the date on your computer, see your Windows documentation. For help setting the active date of processes, see your CA Process Automation documentation. For help setting the active date of process definitions, see the CA Workflow IDE online help.

4. Verify the following:
 - Verify that you have enabled the rule actions for updating the request status of interest.
 - Verify whether Message Queue 4.1 Broker and other Windows services mentioned in the next step are running.
 - If you are using CA Process Automation to manage the request status change of interest, do the following: Verify the configuration parameters (especially the host name, port number, and other connection parameters) for CA Process Automation. Verify especially that the Global Data Set parameter points to the correct Service View computer.

Note: For information about setting the configuration parameters in CA Process Automation, see the *Integration Guide*.
 - If you are using CA Workflow to manage the request status change of interest, [set the CA Workflow configuration parameters](#) (see page 121). Verify especially that the CA Workflow actors point to the correct Service View computer.
 - Verify whether the assignees for the request are members of CA EEM groups whose names include special characters.

If the assignees are members of such groups, the request statuses can fail to update. If necessary, rename the applicable groups in CA EEM so that their names do *not* include special characters.

Note: For information about using CA EEM, see the *Integration Guide*.
5. Restart the CA Service Catalog Windows services. They are CA Service View, CA Service Accounting, CA Service Fulfillment, and Message Queue 4.1 Broker.

Sorting of Services by Selection Type

Symptom:

When I view services in the catalog, they are not sorted by Selection Type as I expect them to be. This observation applies to all services, including the services that appear in the Featured Services section.

Solution:

When you create a service, you specify a Selection Type. The sorting of services according to Selection Type is controlled internally. The sort order is *not* based on the name of the Selection Type. Instead, the sort order is based on the *numeric value* of the Selection Type, as follows:

No Selection

Single Selection

Multiple Selection

Service View Installation or Upgrade Fails Because Path Name is Too Long

Symptom:

During the installation or upgrade of Service View, CA MDB is installed or upgraded automatically. The Service View installation or upgrade can fail while attempting to install or upgrade the MDB, displaying a message similar to the following:

Configure SQL Server or Oracle MDB Failed. The installation will terminate.

Solution:

The maximum length of a path name in Windows is 260 characters. The installation or upgrade can fail if the pathnames it uses exceed this limit. For example, pathnames that include several long, nested folder names can violate this limit.

Verify that the path name where you store and access the CA Service Catalog installation files does not exceed the maximum length.

Similarly, verify that the path name on which you install these files does not exceed the maximum length.

Service View Installation or Upgrade Fails Because of Duplicate Records

Symptom:

During the installation or upgrade of Service View, CA MDB is automatically installed or upgraded.

For example, if CA MDB r1.0.4 is installed, it is automatically upgraded to CA MDB r1.5 during the Service View installation or upgrade. However, suppose CA MDB r1.0.4 is shared with other CA products. In that case, the CA MDB upgrade can fail if duplicate records exist where the CA MDB tables require unique constraints. Examples include the following tables: `ca_resource_class`, `ca_resource_family`, `ca_discovered_software`, `chgcats`, and `cr_stat`.

Solution:

Back up these tables, evaluate them, and clean up any duplicate records in them. Then try again to install or upgrade Service View.

Service View Windows Service Does Not Start

Symptom:

The Windows service for Service View fails to start. This service is named CA Service View.

Solution:

The CA Service View service is set by default to start automatically after a reboot or shutdown. If this service fails to start after a reboot or shutdown, verify that its dependent services are started. Its dependent services are Message Queue 4.1 Broker and iTechnology iGateway.

Start the dependent services first, and then start the CA Service View service.

CA EEM Installation on 64-Bit Operating Systems

Symptom:

This issue applies when you install CA EEM r8.4 on 64-bit operating systems. If you have previously installed CA Threat Manager, it may fail to work properly after you install CA EEM.

Solution:

Prepare to install CA EEM *before* you install it.

To prepare to install CA EEM

1. Verify whether you installed CA Threat Manager as a 64-bit application and proceed as follows:
 - If No, skip the remaining steps.
 - If Yes, complete the remaining steps.
2. Uninstall CA Threat Manager as a 64-bit application.
3. Install CA Threat Manager as a 32-bit application.

After you complete the previous steps, you are ready to install CA EEM.

CA EEM Upgrade Fails

Symptom:

The CA EEM upgrade can become stuck and fail.

Solution:

The typical cause is the presence of CA Threat Manager. To fix the problem, do the following:

1. Uninstall CA Threat Manager.
2. Upgrade CA Service Catalog and CA EEM.
3. Reinstall CA Threat Manager.