

Crystal Analysis Professional

Data and File Security Options White Paper

Overview

This document details security options available for Crystal Analysis Professional (CA Pro). It covers the security model for designing and viewing applications in the CA Pro Designer as well as security options when viewing CA Pro reports over the web through Crystal Enterprise and its eBusiness framework.

Contents

INTRODUCTION	2
CRYSTAL ANALYSIS PROFESSIONAL DESIGNER.....	2
<i>Data Security.....</i>	<i>2</i>
Connecting to the OLAP source.....	2
<i>Design Security</i>	<i>3</i>
CRYSTAL ENTERPRISE SECURITY FOR CA PRO FILES	3
<i>Crystal Enterprise Security Options.....</i>	<i>3</i>
CONTACTING CRYSTAL DECISIONS FOR TECHNICAL SUPPORT	5

Introduction

Crystal Analysis Professional analytic reports are created using the Crystal Analysis Professional Desktop Designer. These reports can be distributed for desktop viewing to any user with the designer installed or they can be published for distribution through Crystal Enterprise. As a special offer the Crystal Enterprise Standard edition is included with Crystal Analysis Professional for the first five concurrent web viewer licenses. Crystal Enterprise Professional can be purchased as an upgrade from Crystal Enterprise Standard for increased security and control over user rights.

- The CA Pro Designer has two levels of security options: NT Authentication and Locked Design mode.
- Crystal Enterprise offers three different security options for publishing CA Pro analytic reports. The security options all relate to the logon ID used to access the specified OLAP data source.

Crystal Analysis Professional Designer

Data Security

Crystal Analysis Professional allows users to create Analytic Applications from existing OLAP data sources. Users do not have the option to create cubes or save data within the .CAR analytic report file generated by CA Pro.

Connecting to the OLAP source

When designing CA Pro analytic reports the designer establishes a dynamic connection to the OLAP source. As a result, the user is seeing live data as they are creating the CA Pro report. When designing or viewing a completed analytic report from within the CA Pro Designer **NT authentication** is used to establish a connection to the OLAP server.

MS OLAP Server v7.0 and 2000

CUB Files – These are offline cube files that can be used as a data source for CA Pro analytic reports. Security is not maintained within these files, therefore as long as the user has rights to read the physical file they will be able to design and view a report based on the .CUB file.

OLAP Server – Role security can be applied to the OLAP Server to restrict user access at the cube level as well as specifying data restrictions within cubes. Since the Role security is a server function please refer to Microsoft documentation for more details.

iCubes (MS OLAP 2000 only) – iCubes are a new feature in SQL Server 2000. They enable http connections to cubes on an OLAP server. The role security described above applies to iCubes as well.

NOTE	Often users are added to the OLAP administrators group within the operating system's User/Group maintenance. However, subsequently MS OLAP role security may be applied to restrict the users' access to data. In order for the newly defined Roles to apply these users must be removed from the OLAP Administrator's group.
-------------	---

Drill-through data Security

Drill-through functionality is only supported by MS SQL OLAP Services 2000. Drill-through enables users to view a result set of the source data for a specified cell within a cube. Although this is a very powerful feature, organizations may wish to restrict a user's ability to access drill-through. By default this feature is disabled on the OLAP server and can be enabled through permissions in cube roles.

Design Security

File Locking – The CA Pro Designer enables users to lock their application files. This feature disables all design capabilities including the addition of analytic report pages, analysis objects and the modification of an object's size and properties. Users of a locked file can still perform data analysis or navigation functionality that is enabled in the .CAR file.

- Designers have the option to lock the .CAR file with a password.

NOTE	File locking only restricts design capabilities. It does not create a file with saved data or restrict access to data. A locked .CAR file still establishes a live connection to the OLAP data source, therefore reflecting any data changes that may have occurred since design time.
-------------	--

Dimension Restrictions – The Worksheet, Dimension Group and the Dimension Explorer have object properties that can be set to restrict access to rows, columns and paged dimension panels as well as member selectors.

Crystal Enterprise Security for CA Pro files

Crystal Enterprise Security Options

Similar to Crystal Report files, CA Pro analytic reports can be published to Crystal Enterprise folders for distribution via the web. Within CE's Crystal Management Console (CMC) component under Content Management, a data source Username and Password can be specified by analytic report object. Modification of the specified data source logon is done in the Data Source Logon tab for the analytic report object. In addition to the file security offered through this managed environment there are three additional levels for personalizing user rights available through Crystal Enterprise Professional. These levels determine the credentials used to connect to the OLAP data source when viewing a .CAR file. Since CA Pro analytic reports do not have an option to be saved with data, they must be designed taking into consideration the security that has been implemented on the OLAP Server.

Logon using Web Component Server credentials – By default when an analytic report (.CAR file) is published to the Crystal Enterprise (CE) framework it is configured with the same OLAP Server logon used by the Web Component Server (WCS) service. The WCS is the component of the CE framework that connects to the OLAP data source. Utilizing this default logon setting will work when the WCS is installed on the same machine as MS SQL Server Analysis (OLAP) Services so that the OLAP Server accepts the Local System Account as a logon. If the WCS and MS SQL Server are not installed on the same machine the WCS logon can still be used but the Logon for the WCS Server will need to be changed to a specific user account that has the proper rights. Keep in mind that having all users log on to SQL Server Analysis (OLAP) Services under a single logon should only be done in a very generic reporting environment. To make changes to the WCS logon, open the Windows NT or 2000 Services Manager under Administrative Tools, select the Crystal Web Component Server and click on the logon tab under Properties. (Refer to the Crystal Analysis Professional Architecture white paper, CAP8_Architecture.pdf, for more details on the CE components. This document is available at: http://support.crystaldecisions.com/communityCS/TechnicalPapers/cap8_architecture.pdf.)

Logon using specific credentials – One method of applying varied access rights across different users or groups, when a generic level of role security has been implemented on the OLAP server, is to specify object level usernames and passwords. This is applied at an object level and is not a generic setting for all published .CAR files. Using this method, a generic report can be created once and published to different CE folders, which are accessible by different CE user groups. Each report object would utilize a different logon and thus yield a different set of results.

NOTE	Augmenting the MS OLAP security through restricting access to reports in different folders for user groups must be done using Crystal Enterprise Professional. (Crystal Enterprise Standard, included with CA Pro, adheres to the OLAP logon security but does not distinguish between Crystal Enterprise users or groups)
-------------	--

Secondary logon for each application – This option can also be set in the CMC at an analytic report object level. With this option every time the analytic report is requested for viewing the user is prompted to logon to the server with their SQL Server OLAP logon information. (This prompt may not be favorable to all organizations – as an alternative you can also trap the OLAP logon dialog and provide the username and password through CSP code.) This enables the design of a generic report for multiple users that makes use of user role level security implemented on the OLAP server to personalize the data results available for viewing.

All of these logon approaches to SQL Server Analysis (OLAP) Services can be enhanced at analytic report design time by restricting dimension panels and member selectors through the object properties.

NOTE	Again, when publishing report objects for viewing by specific CE user groups Crystal Enterprise Professional must be used. (Crystal Enterprise Standard, included with CA Pro, adheres to the OLAP logon security but does not distinguish between CE users or groups.)
-------------	---

Contacting Crystal Decisions for Technical Support

We recommend that you refer to the product documentation and that you visit our Technical Support web site for more resources.

Self-serve Support:

<http://support.crystaldecisions.com/>

Email Support:

<http://support.crystaldecisions.com/support/answers.asp>

Telephone Support:

<http://www.crystaldecisions.com/contact/support.asp>