Crystal Enterprise 8 Security Concepts

A security view of Crystal Enterprise for the administrator

Overview

This whitepaper walks through enterprise security concerns and how Crystal Enterprise 8 addresses them. It is intended to provide system administrators or system architects with answers to typical concerns regarding security. For those who enjoy details, this document will at times delve into implementation specific settings and overall design of certain components. Some questions that this document intends to answer are: How is security handled in Crystal Enterprise? Does Crystal Enterprise support 3rd party users and group lists? How do I control access to my system? How do I prevent unauthorized entry into the system?

It is assumed that the reader has a basic understanding of the Crystal Enterprise architecture and its components. For more information on Crystal Enterprise architecture, please consult the Crystal Enterprise Administrators Help guide.

Contents

Introduction

The Crystal Enterprise System Platform is the backbone for all enterprise-based Crystal products. By understanding the security features and related functionality provided via the Crystal Enterprise System Platform, one will simultaneously be able to understand how Enterprise-based Crystal products address security-related concerns.

Crystal Enterprise's architecture looks to address the many security concerns that require solutions in the 'open' world we live in. The current release supports features such as Single Sign On (SSO), resource access security, NT authentication, and protection against unauthorized access. In addition, Crystal Enterprise provides built-in encryption support for passwords and private information to ensure that the system is secure. Besides data security, Crystal Enterprise provides monitoring information to track user's actions, thus providing a way to detect potential intrusions.

The following is a list of security related areas that are explained in this document:

- **Security Manager** is responsible for managing security in Crystal Enterprise.
- **Authentication** is the process that verifies the identity of a user attempting to access the system.
- **Authorization** is the process that determines if a user can apply an action on a resource.
- **Active Trust Relationship** describes how the system appears to only require the user to logon once.

- **Session Tracking** monitors the user's state while they are interacting with the system.
- **Environment Protection** is the security applied to the connections and environments that interact with Crystal Enterprise.
- **Auditing** records system information and provides insight into the system's usage and performance.
- **Malicious Logon Attempt Protection** are features that provide ways to deter a malicious user from breaking into the system via the logon mechanism.

Security Manager

In any security system, there are three components: Authentication, Authorization and Aggregation, with Aggregation being a component of other two. In Crystal Enterprise, the Security Manager provides support for the above three A's when communicating with the internal system and accessing external resources linked from the system. The following section provides an introduction to the architecture of the Security Manager, and then a breakdown of how the Security Manager addresses the 3 A's of security.

Architecture

The Security Manager is responsible for managing access to Crystal Enterprise and to specified Crystal Enterprise objects, as well as for providing support for 3rd party security systems. The Security Manager is a Crystal Enterprise service that is transparent to the user but accessible via the SDK. The two primary tasks the Security Manager performs are:

1. Verification that the user is who they claim to be.
2. Determining which resource(s) can be accessed by a particular user.

The first task occurs when a user logs onto the system; the second can occur when a user attempts to view a folder or another object. In addition to handling user requests, the Security Manager also serves as a resource for Crystal Enterprise servers to validate users for tasks and access to resources.

Security Plug-Ins

A Security Plug-In is a component that identifies users and groups for the Security Manager. One purpose of the Security Plug-In architecture is to allow plug-ins to be implemented so that 3rd Party systems' users and groups may be mapped into the Crystal Enterprise security system. This allows administrators to set up users and groups in an external system, and to have those users and groups receive an identity in Crystal Enterprise. To this effect, the Security Manager and the Security Plug-Ins cooperate to bring security to Crystal Enterprise. Another purpose of the Security Plug-In architecture is to allow new plug-ins to be quickly and easily implemented, and dropped in place at any time.

Crystal Enterprise Plug-In

The Crystal Enterprise Plug-In is the default plug-in that ships with the system. The Plug-In allows users and groups to be created and maintained inside Crystal Enterprise.

3rd Party Plug-Ins

A 3rd Party plug-in can access 3rd Party security system's user and group information. That is, 3rd party users and groups can be recognized in Crystal Enterprise for authentication and authorization purposes. For example, Crystal Enterprise allows NT users to log onto the system using their existing NT credentials.

In order to recognize 3rd party users and groups, the Security Manager supports the notions of mapping and importing. Mapping allows 3rd party groups or single users to be mapped to Crystal Enterprise users or groups. Importing allows a direct image of the 3rd party system to be reflected in Crystal Enterprise. With respect to setting rights, mapped or imported users and groups are treated the same as any Crystal Enterprise user or group.

The following scenario illustrates the use of mapping and importing NT users and groups into Crystal Enterprise.

An administrator wants to create a Crystal Enterprise system that consists of two types of users:

- Report Creators are responsible for creating reports.
- Report Viewers who view the reports generated by the Report Creators.

The intent of the system is that the Report Creators will take templates and samples from the shared area to create reports which they store in their own area and then once complete, move them into a common area such that the Report Viewers users can look at them.

The folder structure of the system will contain the following:

- Unique folders for the Report Creators
- A common area that Report Creators post their reports to when done, and which any Report Viewer can view.
- A Report Creator shared area that contains base templates and samples for all Report Creators.

All the users exist in an NT domain. As there are many Report Viewers, the Crystal Enterprise admin doesn’t want their identities to consume Crystal Enterprise system resources. However, the Crystal Enterprise admin still wants to authenticate each login via the NT domain.

NT Setup

- Create the “Report Creators” group and move the users that will be creating reports into it.
- Create the “Report Viewers” group and move the users that will be viewing reports into it.

Crystal Enterprise Setup

The administrator will do all the administration via the Crystal Management Console. In the CMC do the following,

- Under Authorization, NT
- Add the NT "Report Creators" and "Report Viewers" groups.
- Under Users
- Create the "General User" account and using the alias feature; assign all the "Report Viewers" to it.
- Under Folders create the following folders and set the rights on the groups specified.

Folder	Group	Right
Shared	Everyone	No Access
	Report Creators	View
Common	Everyone	View

The setup is complete. As the "Report Creators" weren't mapped to a user, the Crystal Enterprise will automatically create a user account with a home folder in the system for each of them. Additionally, if any users are added or removed from the NT "Report Creators" or "Report Viewers" group, those changes will be reflected in Crystal Enterprise automatically.

As mentioned above, the Crystal Enterprise administrator can manage 3rd party user and groups as if they were Crystal Enterprise users and groups. This allows security to be consistently applied among all security plug-ins. It also makes it easier for administrators to manage changes in external groups and users without corrupting the permissions in Crystal Enterprise.

3rd party user and group synchronization is maintained by the Security plug-in. This means that, if a user of the external system is added to an external group, that change would be reflected in Crystal Enterprise.

Authentication

Authentication is the mechanism used to verify the identity of a user attempting to access the system. The first time a user attempts to access the system is called the Initial Identification. This process involves the user being authenticated against one of the authentication providers. Once the user's credentials have been successfully verified, the user is given an active identity in the system. Secondary Identification occurs at all other times when the user attempts to access the system; their active identity is used to authenticate the user. When the user is finished their work and logs out of the system, their active identity is removed.

An added feature that can be provided by the authentication provider is Single Sign On (SSO). SSO allows a user to enter their logon credentials once and be logged onto multiple systems.

Initial Identification

The process of initial identification is commonly referred to as "logging onto the system". When a user attempts to logon to the system, they specify their credentials (such as username, password), which the system will attempt to verify. Upon successful verification of the user's credentials, the user is granted access to the system; otherwise, access is denied. The security system does not directly verify the user's credentials; instead, it forwards the request to an authentication provider to verify. The Authentication provider in turn will verify the information and reply back to Crystal Enterprise whether the user has been verified or not. After successful verification has occurred, Crystal Enterprise creates an internal active identity for the user. The client component will cache the active identity in the form of a logon token and pass this to Crystal Enterprise when it attempts to access resources in the system.

In a SSO situation the credentials will be retrieved by other means and automatically log the user on without their knowledge.

Secondary Identification

When a client attempts to access a resource in the system, their logon token is passed to the system and secondary identification occurs. This is similar to logging onto the system again, except that Crystal Enterprise does a quick lookup on the logon token. The benefit of the quick lookup is that the system does not have to revisit the Authentication provider for every request, which could be very time-consuming performance hit.

Logon User Scenario	A user wishes to view a report. They are given a web link to a report stored on a Crystal Enterprise installation, which they attempt to access by clicking the link. Crystal Enterprise will attempt Initial Identification, which could result with the user receiving a logon box (or perhaps unnoticeable to the user if SSO is used). Assuming successful logon, Crystal Enterprise will give the user an active identity in the form of a logon token. Crystal Enterprise would then forward the logon token, along with the view request, to the report viewing mechanism. The report viewing mechanism will then verify the logon token and present the user with the report.

Authentication Providers

The Authentication provider is a component of a Security Plug-In. It is the component that allows Crystal Enterprise to verify users' credentials against a database of user information. The Authentication provider is only used during Initial Identification, as the process it uses can be slow and lengthy, and in most cases, uncontrollable by Crystal Enterprise. As Crystal Enterprise supports 3rd party Authentication providers, the speed of the authentication is dependant on the 3rd party implementation of the authentication mechanism. Additionally, if many users are attempting to use the system, the Authentication provider could become quite busy or fail due to too many requests. There are two types of Authentication providers currently shipping with Crystal Enterprise: They are the system default Crystal Enterprise Authentication Provider and NT Authentication Provider.

Crystal Enterprise Authentication Provider

When a user selects Crystal Enterprise Authentication at logon time, they are authenticated against the Crystal Enterprise user list and allowed/disallowed access to the system based solely on that information.

Crystal Enterprise supports the SSO feature. When the user logs on without specifying a username and/or password the system will automatically log them on as a guest.

NOTE	Crystal Enterprise SSO is only compatible with the guest user. To create an identity and an account in the system the user is allowed to create a new user account and then log in as this new user.

NT Authentication Provider

When a user selects NT Authentication at logon time they are authenticated against the NT user database. The provider can be set up so that specific NT groups are mirrored in Crystal Enterprise. The mirrored group's users will exist in Crystal Enterprise as users. The provider also manages synchronization between the Crystal Enterprise system and the NT system, thus reducing administrative overhead for NT user account additions or removal etc.

NOTE	The NT Authentication provider is compatible with NT4 or Window 2000 Active Directory user databases.

NT SSO allows an NT user to logon to Crystal Enterprise from a Windows system without directly specifying their credentials. NT SSO can be utilized by a thick-client or through a web browser.

In the thick-client case, the user must be running on a Windows platform and using the Crystal Enterprise SDK. At log on time, the NT Security Plug-In will query the operating system for the currently logged on user's credentials and use these to authenticate.

To utilize NT SSO in a web scenario, the system must be set up to use all Microsoft components. More specifically, Internet Explorer on a Windows system, connecting to Crystal Enterprise via IIS.

The browser and web server will engage in NT Challenge response to authenticate the user to the web server. Once this is done, the web server impersonates the user to log on to Crystal Enterprise. The rest of the case is similar to the thick-client scenario, where the NT Security Plug-In queries for the user's credentials and utilizes these to authenticate.

NOTE	IIS will perform the NT Challenge response for every web page viewed; this can result in severe performance degradation.

Refer to the Crystal Enterprise Administration documentation on how to configure the components for NT SSO.

Authorization

Authorization is the process that determines which actions a user can perform on a particular resource. Similarly, authorization prevents unauthorized access or actions to occur on a resource without the appropriate permissions being set.

Example	Consider the scenario when a user attempts to view an object residing in Crystal Enterprise. The user selects the objects, selects the view action and hits go. The request is sent to the server. The server finds the object and then performs authorization by checking the rights associated with the object. On success, the server returns the object to be viewed; on failure, the user receives the appropriate error message.

To prepare a secure system, the administrator will need to build a conceptual security view of that system. To a single user, this view is what objects they can see, and what actions they can perform. To an administrator, this is the complex network linking all users, rights and resources in a system. For an enterprise system, building the security view will be one of the administrator's largest tasks.

A goal of most advanced enterprise security systems is to empower the administrator with the ability to provide a high degree of control, while at the same time providing a simple and efficient way to achieve it. In other words, Crystal Enterprise strives to make the building and maintenance of a powerful complex security view as easy as possible. The above is addressed by providing four key areas of authorization-related functionality. They are as follows: Groups, Inheritable Rights, Net Rights, and Access Modes.

Groups

A Group is a set of users and groups. It provides a convenient way of assigning a set of rights to many users. When setting access permissions for an object, the administrator can set the rights to apply to a group of users as opposed a to assigning rights to each individual user. Crystal Enterprise also supports subgroups. Subgroups allow multiple levels of groups to be used to better reflect real-world group scenarios. Additionally, Users and Groups can be in multiple unrelated or related groups, further reflecting real-world scenarios.

Inheritable Rights

Inheritable rights are simply two objects in a parent/child relationship such that the effective rights applied to the parent are inherited by the child. This is the folder/object equivalent to the group/user relationship. If an administrator wishes to apply a set of rights to a collection of objects, they would move the objects into a folder then set the rights on the folder. All objects contained inside the folder would inherit the folder's rights.

Net Rights

Once the security view has been created, a common difficulty is to verify a specific group or user access to an object. Crystal Enterprise solves this problem by introducing the Net Right concept. Net rights show the net results of all the rules applied on a specific user or group for an object. Thus, an administrator can immediately see what access a user or group has to an object.

Access Modes

Similar to folder/object and group/user relationships, Access Modes provide an Access Mode/Right relationship. That is a set of rights, grouped together so that they can be applied to a user/object relationship. Crystal Enterprise comes with several Access Modes to reflect the real world model. The Access Modes are as follows:

- View: Allow viewing access to the object
- Run: Allow viewing and scheduling of a object
- Full Control: View, run, delete modify of an object
- No Access: All access denied

NOTE	Access Modes are sometimes referred to as Roles. They contain a collection of rights to simplify the granting of access to a particular resource.

The following is a table of which internal rights each Access Mode maps to.

Right	View	Schedule (Run)	Full Control
See	X	X	X
View	X	X	X
Schedule		X	X
If Owner(Stop)		X	
If Owner(Delete Instance)		X	
Add			X
Create			X
Edit			X
Stop			X
Modify Rights			X
View Rights			X
Delete			X
Delete Instance			X

Active Trust Relationship

It is expected that enterprise systems today don't need to prompt more than once for a user's primary credentials. In the case of SSO, even prompting once is not preferred. Thus, a requirement for systems is that once the user has been authenticated and given an active identity in the system, the user will be known throughout the system and not be required to re-enter their credentials.

Once a user has been authenticated by the system, all their further requests and actions are processed without appearing to authenticate the user again. This runtime characteristic is called the Active Trust Relationship.

Ticket Mechanism

In a simple, single client-server connection, distributed security is not as necessary. However, for complex enterprise systems dedicated to serving a large number of users it can be difficult to be without a distributed security component. To support such features such as load balancing, stateless environments or transfer of trust (to allow another component to act on behalf of the user), the system must be able to support distributed security.

Crystal Enterprise addresses the above issue by implementing a ticket mechanism. Similar to the way Kerberos ticket mechanism functions, the Security System grants tickets to authorize actions to be taken on the user's behalf. In Crystal Enterprise, the ticket is referred to as a logon token.

The most common of uses of the logon token in Crystal Enterprise is via the web. When a user first connects and is authenticated by Crystal Enterprise, they will receive a logon token that is sent back to the browser. When the user makes a new request, the browser will send the logon token back to Crystal Enterprise. This allows the user to connect to different WCS' so that load balancing can be implemented. In the case of report viewing, the browser sends down the logon token to the WCS, which is then forwarded on to the report-viewing server. The report viewing server attempts to logon the user; if logon is successful the report is fetched and returned to the user.

Logon Token

The logon token itself is an encoded string containing information about the user's session information and logon token usage attributes. The usage attributes of the logon token are specified when generation of the logon token is requested. The attributes allow restrictions to be placed upon the logon token to reduce the chance of the logon token being used by malicious users. The current logon token usage attributes are:

- Number of days: The number of days before the token expires
- Number of logons: The number of logons the token can be reused for

The Number of days attribute restricts the lifetime of the logon token. Thus, even if a malicious user retrieved the token, it would be invalid and of no use to them.

The Number of logons attribute, restricts how many times the logon token can be used to logon to Crystal Enterprise. Thus if a malicious user intercepted the logon token and attempted to logon to Crystal Enterprise, they would be denied as the logon token had already been used.

Session Tracking

Sessions are simply some amount of state being stored about a user on a server. Sessions are commonly implemented to increase performance and throughput, as it is common for a user to logon and do a set of independent transactions then logoff. The session allows the system to not have to go through the process of logging on a second time, searching, finding, or redoing any task necessary for the next request. The session should be preserved as long as the user is logged on, however in the web case where interaction with a browser and web server can be stateless, it can be difficult to know when the client has logged off. Additionally, other risks exist, for example if the user left their machine on and went home, leaving the connection open for a malicious user. In both these cases, the system would want to automatically log the user off. Thus to address the above issue Crystal Enterprise implements Session Tracking.

APS Sessions

The APS implements a simple APS Session tracking algorithm. When a user logs on they are given an APS Session and the APS Session is kept around until the user logs off. If the client has not communicated with the APS within a 10 minute (non-configurable) time period then the APS will clean up the APS Session, resulting in the user having to log on again for subsequent requests. However, this case is only to handle times when the client side component shuts down irregularly, as the client is designed to notify the APS on a recurring basis that it is still active and thus should not be logged off. Therefore, as long as the client is running the connection will be valid.

WCS Sessions

The WCS implements Session Tracking similar to the way most web server implement it. That is, if the server side script pages (.csp) programmatically save variables to the WCS Session then the WCS retains the WCS Session for a default of 20 minutes after the last user request. If a .csp page logs onto the APS on behalf of the user then stores this connection in the WCS Session, at the time the WCS Session expires the WCS will log the user off the APS.

Crystal Enterprise is flexible in the use of session state. WCS Session state can be used or not used; it can be used for some of a users requests and perhaps not for the others. The decisions when or when not to use WCS Session state is dependant on the web site requirements. For example, a site that aims to ensure high security may use WCS Session state as it can reduce the amount of sensitive data transmitted via the web. Where as a site that aims to have the fastest response time possible per request may not use any WCS Session state.

USER SCENARIO	If the user connects to Crystal Enterprise via the web, logs on then shuts down the browser without logging off, the APS will record that user as logged on for 20 minutes before the WCS releases the WCS Session and thus releasing the APS Session.

NOTE	The WCS Session timeout can be programmatically configured in the server side csp pages to timeout earlier if the default of 20 minutes is not desired.

For more information about Crystal Enterprise and session use, refer to the Crystal Enterprise Session document.

Environment Protection

A major concern for administrator is that the environments the clients and system run in are secure. Today the least secure scenario involves a user accessing a system via the Internet. As the administrator cannot secure the Internet, the concern is separated into two components with the dividing line being the web server. For Crystal Enterprise these components can be distinguished as the following:

- The area of communication from the web browser to the web server
- The area of communication from the web server to Crystal Enterprise

NOTE	It should be noted that the physical break between the system and the Internet is via an outer firewall. However, from a connection configuration point of view it is easier to discuss the separation at the web server.

Web Browser to Web Server

If the data being transmitted between the web browser and web server does not contain sensitive information no security is required, however in the likely event that the data is sensitive then the administrator will want to ensure security. As the Internet cannot be secured, the administrator must look to other means of ensuring a secure environment. The problem is then broken down into two separate parts:

- Ensuring the data communication is secure.
- Ensuring the user connection to the web server is who they claim to be.

The above are implemented by web servers in various ways; using SSL, challenge response and other such mechanisms. Securing the communication between the web browser and web server can be configured independently of Crystal Enterprise. Thus, the administrator will need to refer to the web server documentation for how to configure secure client connections.

Web Server to Crystal Enterprise

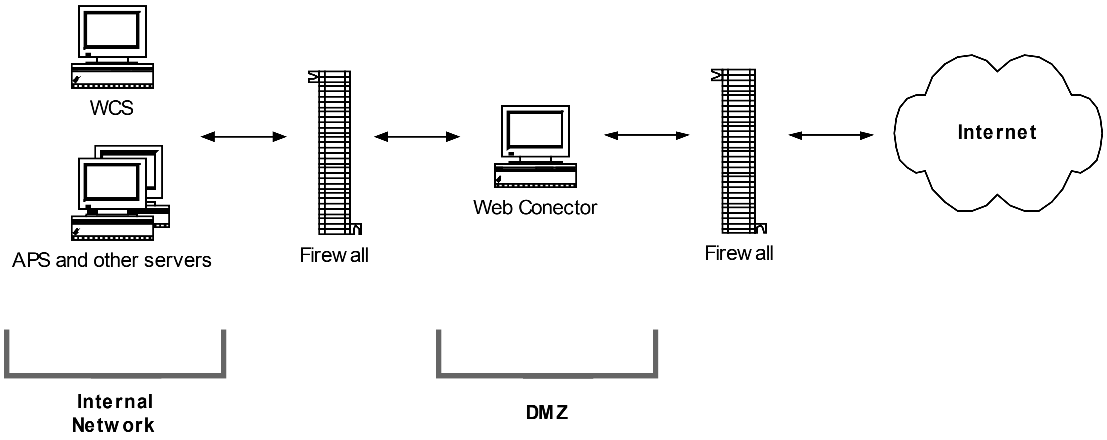
As the area behind the web server is under the control of the administrator, steps can be taken to ensure a secure environment. These steps commonly involve wrapping the area with firewalls.

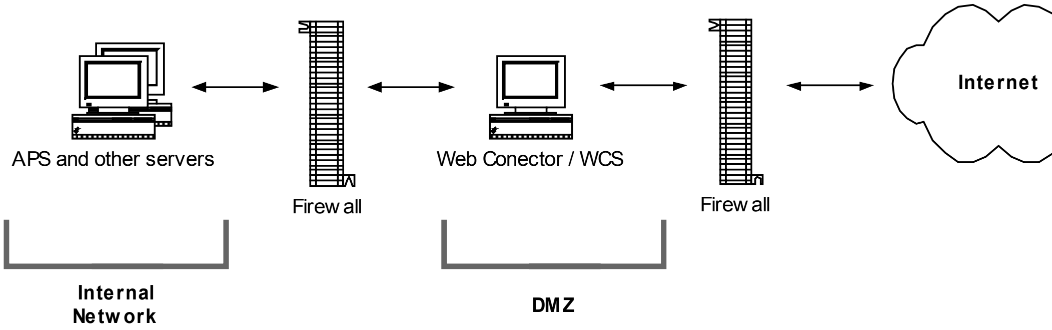
The typical setup for firewalls is to have a corporate outer firewall that separates the corporate web server and the Internet followed by another firewall separating the corporate web server and the rest of the servers in the system.

This area between the two firewalls is commonly referred to as the Demilitarized Zone (DMZ).

Firewalls

Crystal Enterprise integrates with many firewalls and supports a multitude of configurations. The more common implemented scenarios that Crystal Enterprise supports are:





To communicate through the firewalls Crystal Enterprise can be configured to work with either:

- IP filtering
- Socks proxy

Crystal Enterprise integrates with many other scenarios involving multiple firewalls, multiple web servers, and multiple WCSs.

Auditing

As systems become more complex it becomes increasingly difficult to track what is occurring and when. Auditing provides insight into the system; it records basic system and user run-time information such that the data may be inspected to provide a way to monitor the activity of the system.

WCS

Depending on what information is recorded there are many different areas that can be exposed about the system. As Crystal Enterprise is designed for high web interaction, there is a rich set of web attributes available that may be recorded. The WCS monitors actions performed and allows the administrator to configure which information is logged. The actions are logged to disk as text files in a comma-delimited format such the files may be imported and reported off.

Malicious Logon Attempt Protection

No matter how secure a system is there is often at least one point that is venerable to attack. That point can be where valid users are allowed access to the system. It is nearly impossible to protect this point from failure and steps must be taken to reduce the risk. That is simply guessing a valid username and password pair remains to be the easiest and one of the most effective ways to "crack" a system.

Crystal Enterprise implements several techniques to reduce the probability of a malicious user achieving access to the system.

Password Restrictions

To ensure that users enter passwords that are relatively complex, thus making a malicious user's job that much more difficult. Crystal Enterprise implements the two following options:

- Enforced Mixed case password
- Enforced minimum password length

Logon Restrictions

The dictionary attack is a method wherein a malicious user gets a user's ID and exhaustively tries every word in a dictionary of common words in an attempt to learn the password. With the speed of modern hardware today, a program could attempt millions of password guesses in a minute. To prevent this, Crystal Enterprise implements several features to reduce the risk of a dictionary attack. They are as follows:

- Disable accounts after a specified number of failed logons
- Reset failed logon count after a specified number of minutes
- Re-enable an account after a specified amount of time
- An internal mechanism to avoid a dictionary attack puts a ½ to 1 second time delay when a user attempts to logon for a second time.

User Restrictions

To ensure that passwords do not become stale, the Security system can require that they be updated regularly. The main reason for this is to stop someone who has already guessed a password and is now sharing the account without the account owner's knowledge. An additional reason is if a malicious user using a database of possible passwords to "crack" into the system they would have to start over, every time passwords change, reducing their effectiveness. As password changes are based on the user first logon time, it is also difficult for a malicious user to determine when the password will be changed. The User Restrictions options are:

- Require user to change password every N days
- Disallow password reuse for N most recent passwords
- Must wait N minutes to change password

Guest Account Restrictions

In Crystal Enterprise, guest users may be allowed to roam the system. At some point they may want to create an identity so that they can configure their viewer; have their own set of Crystal Reports or Crystal Analysis Professional Objects; add reports to the system etc. Crystal Enterprise provides the option of allowing or disallowing a guest user to create his or her own account.

Finding More Information

For more information, please review the following documentation or contact Technical Support.

Product Documentation

Available in electronic format in the \Doc directory of the Crystal Enterprise CD and on the Crystal Decisions support web site at:

http://support.crystaldecisions.com/docs

- Crystal Enterprise Quick Start Guide (ce8_quick_start_guide.pdf)
- Crystal Enterprise Administrator’s Guide (ce8_administrators_guide.pdf)
- Release Notes (ce8_release.pdf)

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

****

The information contained in this document represents the best current view of Crystal Decisions on the issues discussed as of the date of publication, but should not be interpreted to be a commitment on the part of Crystal Decisions or a guarantee as to the accuracy of any information presented.

This document is for informational purposes only. CRYSTAL DECISIONS MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT. CRYSTAL DECISIONS SHALL HAVE NO LIABILITY OR OBLIGATION ARISING OUT OF THIS DOCUMENT.

Specifications and product offerings subject to change without notice.