ConsoleWorks by TECSys Development

SECURITY TUTORIAL

www.tditx.com

Security Fundamentals

There are a number of security considerations in conjunction with a Console*Works* installation. Mainly, it is important to note that ConsoleWorks does not displace any existing security mechanisms, but rather provides additional opportunity to enhance the enterprise environment for securing managed consoles/devices.

TECSys Development, LP (TDi) is ready to consult and recommend specific configurations to meet the variety of security requirements encountered with a Console*Works* installation.

Security topics covered in this document address:

- Administrator Account
- User Accounts
- User Profiles
- Profile Privileges
- Front Side/Back Side
- Browser Considerations
- Direct Serial Connections
- Console Server Connections
- Private Management Network
- Console*Works* Server Hierarchy
- Failover Server

Administrator Account

The ConsoleWorks Administrator account is a Console*Works* user with the appropriate privileges to administer the Console*Works* server. The default profile with administrative privilege is CONSOLE_MANAGER which has the ability to read, write, control and delete user accounts, profiles, and console/devices.

User Accounts

In order to access the Console*Works* browser interface, a user must have a valid login account. This account is established by the Console*Works* administrator and requires the user to enter a valid username and password.

When setting up user accounts, the Console*Works* administrator defines the user's ability to make changes to his/her own account, the minimum password length for the account, an expiration date for the account, and the profiles that the account can use to gain console access.

Profiles

Profiles define the set of privileges that can be assigned to users within Console*Works*. The two sets of privileges available are called Administrative and Console. Users are granted the use of one or more profiles in order to accomplish the desired tasks. Aspects of a profile are:

- it can contain none, some or all of the privileges available for the Console*Works* server;
- it can contain none, some or all of the privileges available on each defined console within Console*Works*;
- same profile can be used by multiple users;
- multiple profiles can permit access to the same console;
- multiple profiles can be used by a single user, but not concurrently.

Profile Privileges

Console*Works* Administrative privileges grant the necessary access to manage the Console*Works* invocation. These privileges include Read, Write, Delete and Control for server functions (i.e. user accounts, profiles, and consoles/devices.

- **Read** - The ability to read the server configuration database. This allows a profile to look at all configuration information, but not change it.
- **Write** - The ability to update console information such as console, events and users. It does not imply the ability to write to the console.
- **Control** - The ability to control the Console*Works* server, shut it down, access the admin options on the menu panel, expunge events and do other admin related activities.

- **Delete** - The ability to remove ConsoleWorks configuration information. This includes deleting consoles, profiles, users, events, etc.

Console privileges include Read, Acknowledge, Write, and Control for console associated actions.

- **Read** - Allows the user to monitor a console.
- **Ack** - Allows the user to acknowledge active events for a console.
- **Write** - Allows the user to interact with the console, i.e., log onto the system or device through the console port.
- **Control** - Gives the user the ability to purge events from a console and to send protected characters to it.

While the console privileges allow a user to establish a read/write connection to a managed console, it is important to note that Console*Works* does not circumvent any of the existing security associated with that system. In other words, the user attempting to access that system must have a valid account on that system.

Front Side/Back Side

As related to a ConsoleWorks server, the two communications channels are utilized and should be considered in any security discussion. Since Console*Works* is a web server application, the communication from the user's browser and the Console*Works* server is referred to as 'front side' communication. The communication from the Console*Works* server to the console port of the managed system/device is referred to as the 'back side' communication. Further down, you will see basic configurations from software encryption to hardware solutions implemented to address both. Depending on the environment, some combination of both may be appropriate. TDi can assists customers with risk assessment and make recommendations appropriately.

Browser Considerations

Console*Works* is a web server—thus an industry standard browser serves as the user interface (Figure 1). This 'front side' browser-to-server connection utilizes the hyper-text transmission protocol (HTTP) which passes information in an unencrypted format across the network. While this may be acceptable most corporate environments, physical and protocol enhancements are available to tighten the browser communications security.

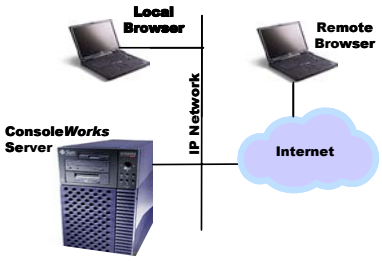

Figure 1

Since remote access to the ConsoleWorks server from the Internet is a useful capability, additional security should be put in place through firewalls and virtual private networks.

Additionally, a Secure Sockets Layer (SSL) SSL Version 3 option (128-bit encryption) is available from TDi.

Direct Serial Connections

Since security on the browser side is one part of the equation, it is important to understand the 'back side' security aspects from the Console*Works* server to the managed device. One way is securing the connection by a direct serial connection between these two (Figure 2).

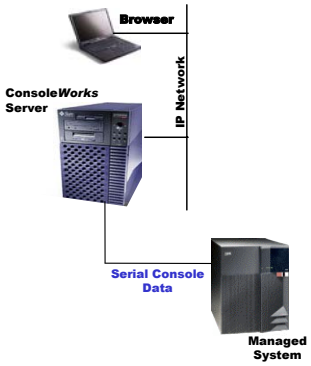

Figure 2

The direct serial connection provides for secured physical access to the serial console port on the managed system. While desirable, this does limit the configuration to the number of serial ports available on the Console*Works* server, and the physical RS232 cable length limitation (approx. 50 feet). This would be suitable to a small data center where all the systems are in close proximity.

Console Server Connections

A console server (sometimes called Terminal Server) is the most popular method for establishing the serial console connection to the Console*Works* server (Figure 3). This 'back side' console connection through a console server is achieved by connecting the console server to the network and connecting the serial cable of the managed device directly to the serial port on the console/device server. Console servers come in a variety of configurations that typically support from 1 to 64 serial connections.

This type of connection has proved to be the most popular connection method, since multiple data centers and an extended geography are easily supported by a single Console*Works* server.

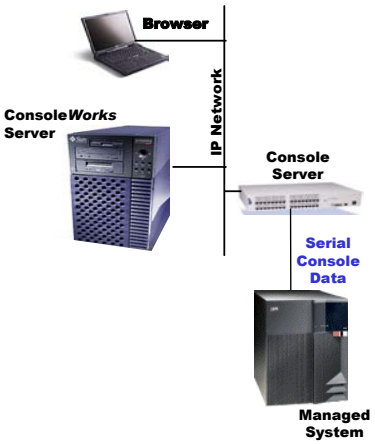

Figure 3

Console servers typically support either Telnet or Local Area Terminal (LAT) protocols. They are assigned a network address allowing Console*Works* to gain access to the individual serial ports using the network address and individual serial port number. The console server ports must be configured to support the speed and characteristics required by the individual system to be managed.

Communication from the Console*Works* server to the managed system console on the network would be either Telnet or LAT. These protocols pass information in an unencrypted format across the network. To secure this link, PseudoConsole connector type and a customer provided SSH (Secure Shell) Client on the Console*Works* server and a SSH-capable Console Server are used.

Private Management Network

Physical network security may be maintained by implementing a private management network (Figure 4) to address 'back side' communication. This hardware-based solution permits the use of non-SSH capable console servers to provide managed system connectivity.

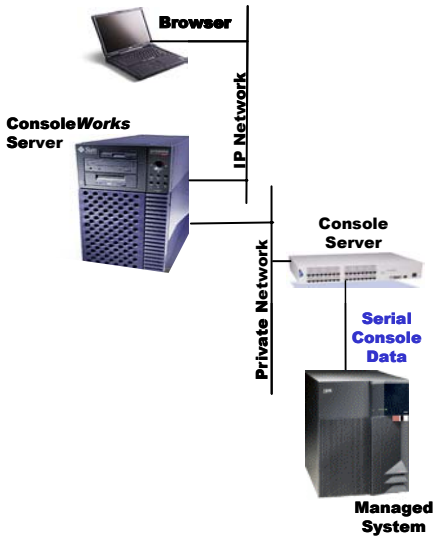

Figure 4

Configuration of the Console*Works* server includes turning off network routing in order to eliminate exposing the private network and its traffic to the standard corporate IP network.

Console*Works* Server Hierarchy

Utilizing the InterServer connector console type, a hierarchy of Console*Works* servers may be configured (Figure 5). The

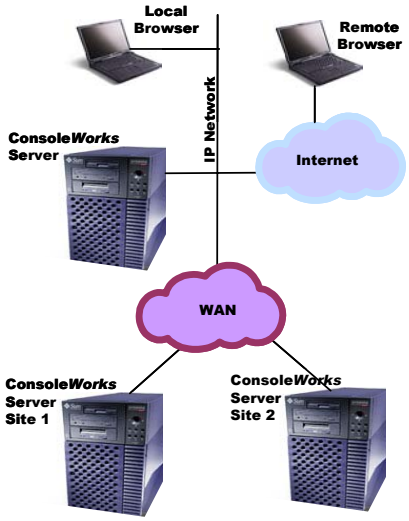

Figure 5

InterServer connector allows the consoles managed by one server to be 'forwarded' to a second Console*Works* server.

This allows remote servers to be 'collected' at a central management point. Potentially more significant is the ability to provide a backup dial-in capability to remote Console*Works* servers if the network between the central management site and the remove site becomes unavailable.

While appearing to be a combination of 'front side' and 'back side' communications, the communication between the Console*Works* servers utilizes the HTTP protocol and represents a 'front side' issue. If encryption of these links is required, then each server should have the Secure Sockets Layer (SSL) option installed.

Remote dial-up capability to remote Console*Works* servers is handled by traditional 'challenge' mechanisms. The ConsoleWorks server can then be administered via a command line interface to assist in restoring normal operations.

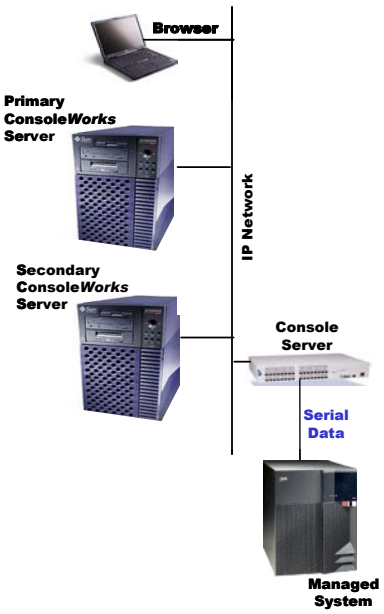

Figure 6

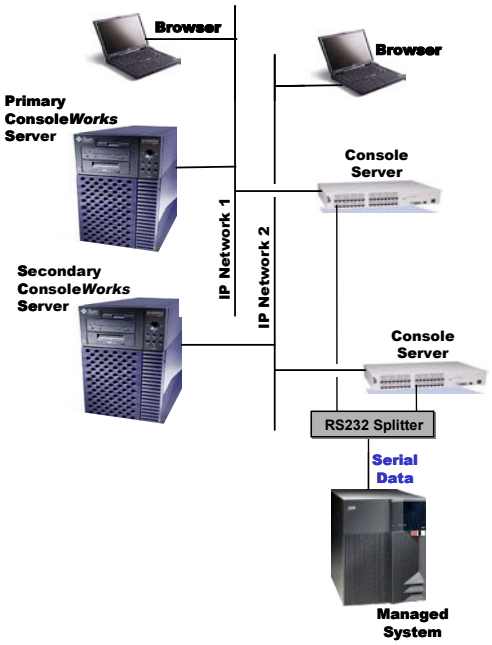

Figure 7

Failover Server

The Failover Server connector type within Console*Works* allows setting up highly available configurations. Connections are established between two servers with console definitions for the same set of managed systems. If one of the servers fails or is not able to establish the 'back side' console communication, the other server takes over.

The Failover Console configurations can be designed to protect against Console*Works* server failure (Figure 6) and/or network failure (Figure 7).

The basic 'front side' and 'back side' communications are addressed with the techniques previously discussed. The failover link between Console*Works* servers is a 'front side' issue. If encryption of these links is required, then each server should have the Secure Sockets Layer (SSL) option installed.

In Summary

Security is a fundamental consideration for any Console*Works* installation and requires careful attention. This brief technical document attempts to provide a basic understanding of the issues and the mechanisms in place.

The examples used in this document address security issues and not necessarily address availability. Please refer to other documents in this series for this type of information.

As with any other installation providing critical business functionality, the importance of the design of your console management solution using Console*Works* is strategic to your success. Since 1994, TDi has helped our customers implement quality solutions within the framework of sound information technology practices.

Need More Information?

For additional product information, design assistance, a live demonstration, or current pricing, please call 1-800-695-1258 or visit our web site at http://www.tditx.com.

World Headquarters
TECSys Development, LP
1600 10th Street, Suite B
Plano, TX, USA 75074-8671
Tel: +1 800.695.1258
Tel: +1 972.881.1553
http://www.tditx.com/

American Headquarters
TECSys Development, LP
1600 10th Street, Suite B
Plano, TX, USA 75074-8671
Tel: +1 800.695.1258
Tel: +1 972.881.1553
http://www.tditx.com/

European Contact
XuiS
The Pavilions
Kiln Lane
Epsom, Surrey, UK KT17 1 JF
Tel: +44 (0) 1372 728881
http://www.XuiS.com/

ConsoleWorks is a registered trademark of TECSys Development, LP.
Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).