Using EMC Unisphere in a Web Browsing Environment: Browser and Security Settings to Improve the Experience

Applied Technology

Abstract

The Web-based approach to system management taken by EMC® Unisphere™ software offers various advantages to EMC Celerra® administrators, such as ubiquitous access and multiplatform support. However, this approach means that Unisphere gives up an element of control over the user's experience. This white paper explains how Unisphere can be affected by the user's browser settings for security and privacy, and it makes setting recommendations for specific versions of Internet Explorer, Mozilla Firefox, and the JRE.

August 2010

Table of Contents

Executive summary

EMC® Unisphere™ software's Web-based approach to system management offers various advantages to system administrators, such as ubiquitous access and multiplatform support. However, compared to native applications, the use of a Web-based approach means that Unisphere gives up an element of control over the user's experience. While an application can directly manipulate its operational environment and thus precisely control a user's experience, a Web-based application depends on several factors within a user's Web browsing environment. A user's choice of the operating system, Web browser, version of the Java Runtime Environment (JRE), and security and privacy settings affects their ability to use the full range of features offered by Unisphere.

Introduction

This white paper explains how Unisphere can be affected by the user's browser settings for security and privacy, and it makes recommendations for specific versions of Internet Explorer, Mozilla Firefox, and the JRE. It covers the following:

- Understanding Secure Sockets Layer (SSL) certificates for the Control Station—how they are generated and how to install them such so that a browser recognizes them seamlessly
- Accepting signed Java applets
- Knowing the difference a browser version makes
- Installing and working with the JRE
- Accepting cookies from the Control Station

For Unisphere to operate properly, a user's Web browsing environment must support the running of Java applets and cookie exchange.

Audience

This white paper is intended for administrators responsible for the overall configuration and operation of Unisphere.

Supported and recommended versions for Web browsers and the Java Runtime environment

Unisphere is designed and tested to work with both Microsoft Internet Explorer (version 6.0 with service pack 2 or later) and Mozilla Firefox (version 3.0 or later). While Unisphere may work with other browsers, support is offered only for the appropriate version of these two Web browsers. In addition, Unisphere requires that version 1.6.0_13 or later of the JRE be installed.

SSL certificates for the Control Station

Communications between a user's Web browser and the Celerra Control Station use Hypertext Transfer Protocol Secured (HTTPS). This allows all HTTP traffic to use SSL encryption. HTTPS prevents sensitive information, such as administrative passwords, from being sent over the network as plain text. During the SSL "handshake" process, where the browser and the Control Station agree on a key for encrypting the session, it is necessary for the Web server on the Control Station to present an SSL certificate to the client browser. When these certificates are encountered on the Web (for example, at an online retail establishment), the certificate is used to positively identify the Web server and generate a session key. These certificates are signed by a handful of recognized Certificate Authorities (CAs) whose identity is built into the browser. Thus, HTTPS provides a verified chain of authentication or trust from a recognized source to that online merchant's Web server. This serves two important purposes: to verify the identity of the merchant (so that customers are assured that they are dealing with a legitimate agent) and to encrypt

session traffic (so that sensitive information, such as a credit card number, is not exposed in transit over the network).

The primary goal of SSL usage for the Celerra Control Station is to protect sensitive information in transit. For this purpose, the Control Station uses self-signed SSL certificates. A self-signed SSL certificate is one that does not have a verified chain of trust back to a CA recognized by a Web browser. This does not diminish the level of the protection afforded to information on the network. However, it does mean that a user's Web browser is most likely going to display a warning about the SSL certificate when it is presented.

The first time a user points the Web browser to a Celerra Control Station, a warning about the SSL certificate appears. The exact warning depends on the state of the SSL certificate installed on the Control Station. This warning will be one of the following:

- The certificate does not match the hostname. If you view the certificate, it is for "localhost.localdomain." This message means that the SSL certificate must be generated and installed. "Generating SSL certificates on the Control Station" on page 11 provides instructions on how to do this.

- The hostname in the certificate does not match the hostname in the URL. This message is typically seen when the URL used to reach the Control Station is not fully qualified or when an IP address is used. For example, if the fully-qualified domain name for the Control Station is hostname.domain.com and the URL merely specifies the hostname, you will see this warning. You can ignore this warning and proceed or reconnect by using the fully-qualified hostname in the future to avoid the warning.

- The certificate was issued by an unrecognized certificate authority. This message is normal for self-signed certificates. If you choose to install the certificate, you will not see this message in the future (from the workstation and browser into which the certificate was installed).

After you complete the login process, Java applets will be loaded into the user's browser. Because the JRE represents a separate runtime environment, it also asks about accepting the SSL certificate from the Control Station.

Understanding the SSL certificate

When a Celerra system is initially installed, a generic SSL certificate is presented, which does not identify the Control Station (it does not have a verified chain of trust back to a recognized CA).

Internet Explorer and Mozilla Firefox will present security alerts and certificate acceptances differently.

Internet Explorer 6.0

In Internet Explorer 6.0, the security alert will appear similar to Figure 1 on page 6.

Figure 1. Initial Security Alert dialog box for IE 6.0

If you view the certificate, you will see that a generic certificate is in place. After the hostname and DNS domain for the Control Station are established, a new SSL certificate should be generated and installed.

After you install a new SSL certificate, pointing a browser at the Control Station should display a dialog box similar to Figure 2 on page 6.

Figure 2. Security Alert dialog box after installing the SSL certificate

Because the level of protection required from SSL is to encrypt traffic and not to establish the Control Station's identity to an arbitrary user, the certificate is sufficient[1]. However, this means that your browser

---

[1] And cheaper, since certificate authorities charge money for their service.

will issue a warning about it. To suppress this warning on the subsequent uses of Unisphere, click **View Certificate**. A dialog box similar to that shown in Figure 3 on page 7 appears.

Figure 3. The SSL certificate

You can click **Install Certificate**, install the certificate, and suppress any SSL-related warnings when pointing a browser to the Control Station. Note that this is required for each browser used to access Unisphere. This means that Internet Explorer must have the certificate installed separately and you need to install it from every client system regularly used to access Unisphere.

Internet Explorer 7.0 and 8.0

In Internet Explorer 7.0 and 8.0, the security alert results in a window similar to Figure 4 on page 8.
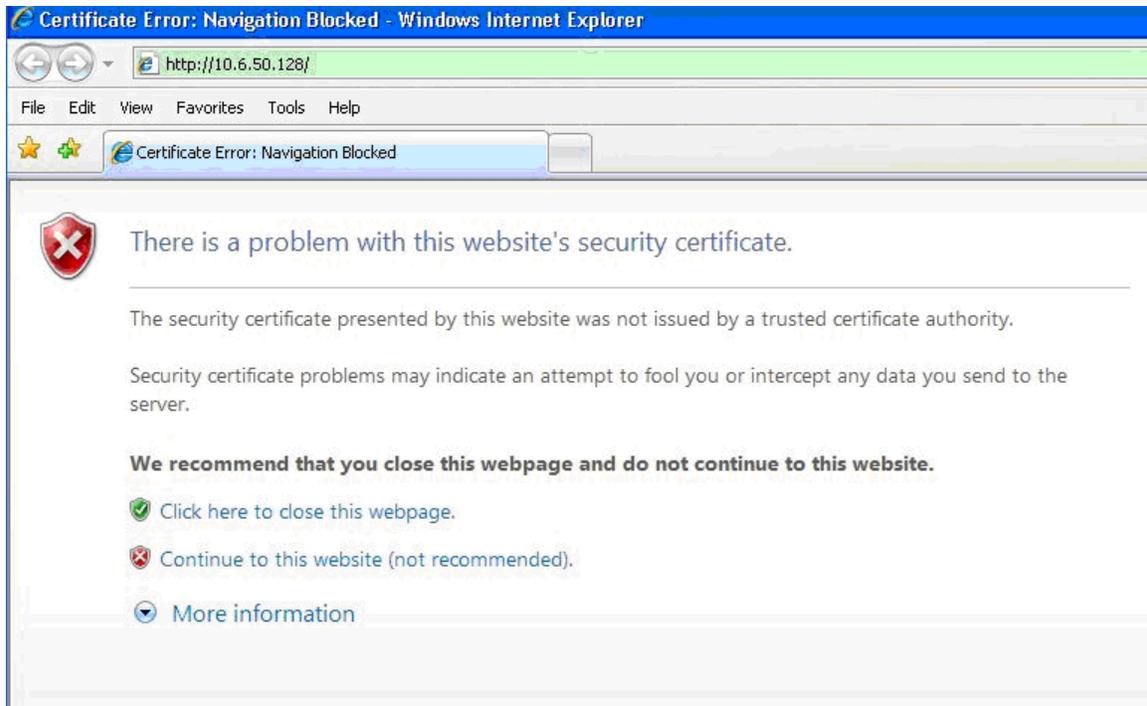
Figure 4. Initial Security Alert window for IE 7.0 and IE 8.0

Select **Continue to this website** because this will allow you to bypass the credential exception. A warning about the certificate will be presented before the exception is bypassed. For Unisphere usage, select **Always trust content from the publisher** and click **Yes** to suppress any further SSL-related warnings as shown in Figure 5 on page 8.
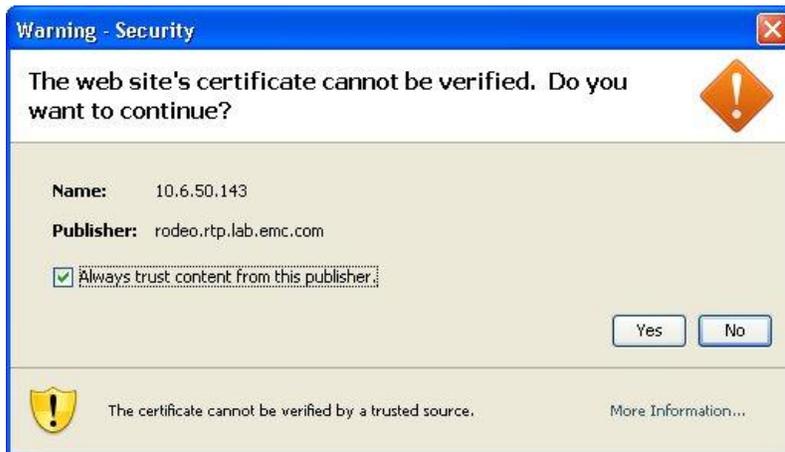

Figure 5. Security warning (certificate)

A similar message appears when it is required to validate the Unisphere application's digital signature (Figure 6 on page 9). Follow the same steps as mentioned above for bypassing the certificates.

Figure 6. Security warning (application)

Accepting this certificate or application signature is also required for each browser that is used to access Unisphere. Each client system that is used to access Unisphere must also install the certificate/signature.

Mozilla Firefox 3.0

In Mozilla Firefox 3.0, the initial security alert results in a dialog box as shown in Figure 7 on page 9. If the details under **I understand the Risks** are not displayed, click **I Understand the Risks** to expand that section.
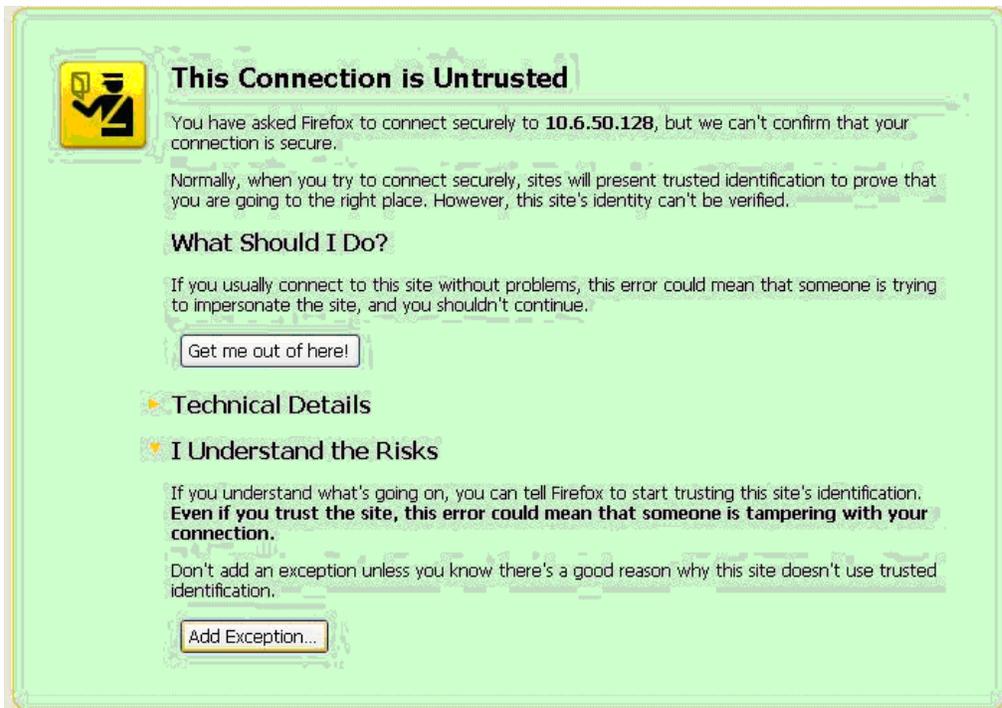

Figure 7. Initial security alert for Firefox 3.0

Click **Add Exception** because this will allow you to bypass the credential exception and accept a self-signed certificate. The user can view the certificate details. To suppress future SSL-warning messages, select **Permanently store this exception** before proceeding (Figure 8 on page 10).
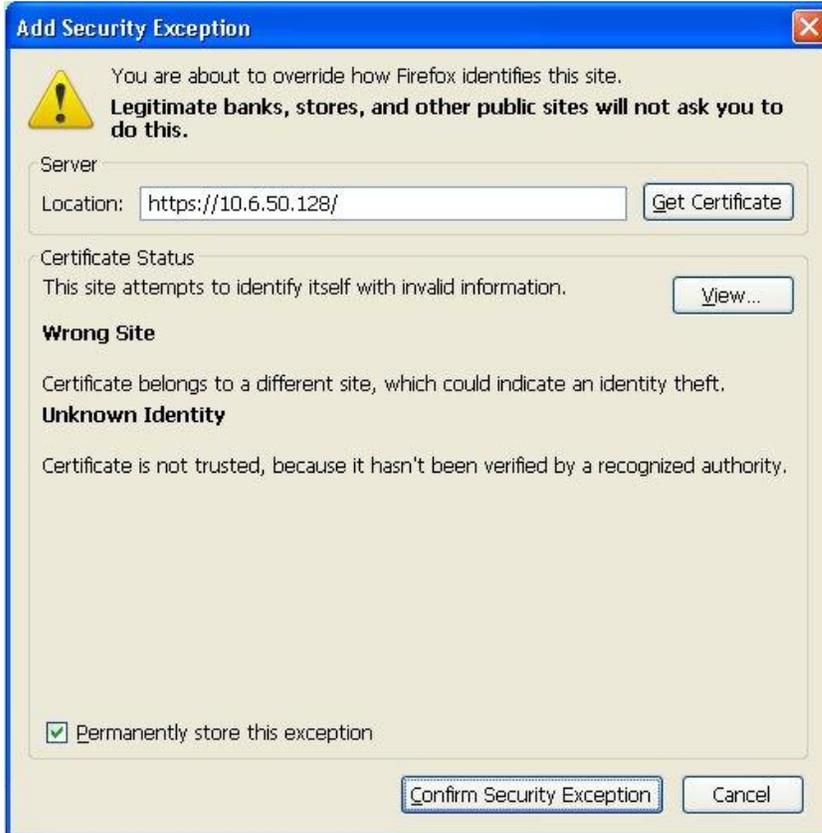
Figure 8. Security certificate acceptance

You may encounter a warning about the certificate, which will be presented before the exception is bypassed and the self-signed certificate is installed. For Unisphere usage, select **Always trust content from the publisher** (Figure 9 on page 10).

Figure 9. Certificate confirmation

A similar message may appear when it is required to validate the signature for the Unisphere application as shown in Figure 10 on page 11. Follow the same steps that were used to accept certificates.

Figure 10. Application confirmation

Accepting this certificate or application signature is also required for each browser that is used to access Unisphere. Each client system used to access Unisphere must also install the certificate/signature.

Generating SSL certificates on the Control Station

After the network interfaces and fully-qualified hostname have been configured for the Control Station, you should generate a new SSL certificate. This does not require any special knowledge of how SSL works or about SSL certificates in general. As the root user on the Control Station, run the following command:
`/nas/sbin/nas_config –ssl`

You will see a warning that the Apache Web server on the Control Station will be restarted.

Example:
```
[root@murano nasadmin]# /nas/sbin/nas_config -ssl

Installing a new SSL certificate requires restarting the Apache web server.

Do you want to proceed? [y/n]: y

New SSL certificate has been generated and installed successfully.

[root@murano nasadmin]#
```

Verifying SSL certificates

Internet Explorer will display a "thumbprint" of the certificate. Review the thumbprint to verify that the certificate that you are going to install came from the Control Station.

To find the SHA1 or MD5 thumbprint of the SSL certificate installed on the Control Station, it is necessary to find the name of the certificate from the file `httpd.conf` located in the `/nas/http/conf` directory. The `openssl` command is used to generate the thumbprint. An example follows:

Example:
```
[root@murano conf]# grep ssl_crt /nas/http/conf/httpd.conf
SSLCertificateFile /nas/http/conf/ssl.crt/ssl_crt.1072810492

[root@murano conf]# openssl x509 -sha1 -in \
/nas/http/conf/ssl.crt/ssl_crt.1072810492 -noout –fingerprint
```

```
SHA1 Fingerprint=36:23:A7:FA:A1:BF:67:F9:24:9B:6A:DD:B8:67:1F:88:D0:D3:AE:30

[root@murano conf]# openssl x509 -in /nas/http/conf/ssl.crt/ssl_crt.1072810492 \ -
noout –fingerprint

MD5 Fingerprint=4E:33:3B:EB:08:16:44:B4:38:A5:B3:03:46:88:BB:F2

[root@murano conf]#
```

Security and privacy settings for Unisphere with Celerra

Cookies and session tokens

In the Web, a *cookie* is a small bit of information that a Web server asks a browser to store locally. Typically, this is done to maintain some kind of state or history between subsequent visits to a website, whether the time between those visits are spaced seconds, minutes, days, weeks, or months. Because HTTP (and by extension, HTTPS) is a stateless protocol, every interaction with a Web server is actually separate and distinct. When a browser returns a cookie to a Web server, this helps the Web server to create a session or to provide some continuity within a visit to a site.

The Celerra Control Station's Web server uses cookies to implement session tokens. Because session tokens are an integral part of how the Unisphere login process works, a user's browser must be configured to accept cookies from the Control Station in order to use it. Depending on the browser that is used and the underlying operating system, this may be an invisible and seamless operation. However, it may be necessary to make changes to a browser's security and privacy settings to accept cookies from the Control Station.

The most likely issue with any login difficulties (assuming a valid username/password pair) is with the browser accepting cookies from the Control Station. Whether a browser accepts a cookie presented to it depends on the security and privacy settings for the browser and, for Internet Explorer, within which *zone* the Control Station is considered to reside.

Session tokens

Session tokens are HTTP cookies that are used to identify a user after the user credentials have been authenticated by the system. The session tokens identify information such as the username, the source IP address, and how long the session token is considered valid. They do not contain any sensitive information and are cryptographically checksummed to prevent modification. Session tokens are either persistent or nonpersistent, based on how the Control Station is configured. Persistent session tokens are stored on the remote system and allow the holder to monitor the system status for extended periods of time with tools such as Celerra Monitor. Nonpersistent session tokens are not stored and are automatically deleted by a browser once the browser session is terminated. The *Celerra Security Configuration Guide* explains how to protect session tokens.

Configuring browsers for Unisphere

Internet Explorer (for versions prior to Windows Server 2003)

The steps to configure Internet Explorer optimally for Unisphere depend on the version of Windows that is running on the client system. Because Windows Server 2003 has enhanced security and privacy settings and uses a more conservative set of defaults, configuring Internet Explorer for that platform will be different from configuring it for other versions of Windows.

Depending on the zone in which the Control Station resides with respect to the client system, different steps may be required to accept cookies. The zone is one of the following:

- Internet
- Local intranet
- Trusted sites
- Restricted sites

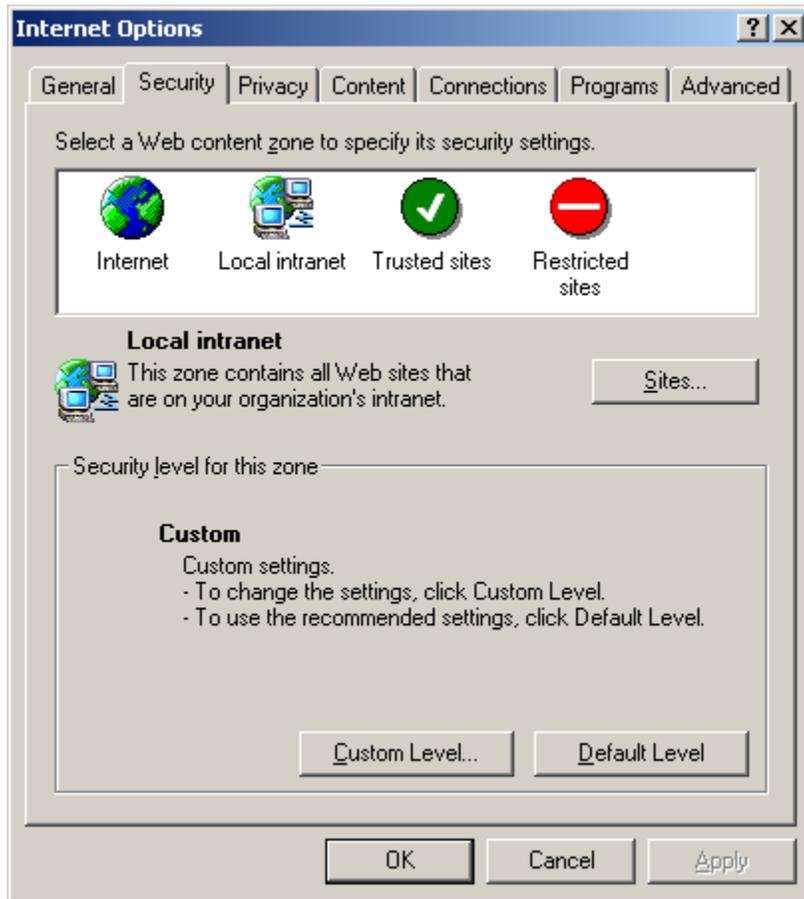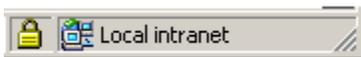Zones are configured on the **Security** tab of the **Internet Options** dialog box as shown in Figure 11.

Figure 11. Security tab of Internet Options

If the Control Station is recognized in the local intranet zone (as indicated by the following figure in the lower right-hand corner of the browser), then you do not need to do anything else to have cookies accepted.

However, there are some situations where a system will be within the local intranet from the perspective of network topology, but it is not recognized as such by Internet Explorer. The most common reason for this to happen is that an IP address is used to point the browser to the Control Station. In this case, the Control Station is considered to be in the Internet zone, as indicated by the following figure.

If you have tightened the default privacy settings, it may be necessary to change settings to accept cookies from the Control Station. To avoid making changes that affect other sites visited on the Internet, the most straightforward thing to do is add the site to the list of trusted sites. To do this within Internet Explorer:

1. Select **Tools** > **Internet Options**.

2. Within the dialog box, click the **Security** tab, and then click the **Trusted Sites** icon.

3. Click **Sites** to add the appropriate IP address. This will allow cookies to be accepted from the Control Station.

A system can also appear to be in the Internet zone when you have used the MCM feature of Unisphere to add a new Control Station to the list of Celerra systems to monitor by IP address or by a non-fully qualified hostname. In this situation, the newly added Control Station address will be considered a *third-party* source for the cookie and these are often blocked by default or with common browser settings. This may look like a failed or looping login attempt after adding the new Celerra system. After authenticating to the new Control Station, you will see the login screen again. There are two somewhat subtle indications that this is not a failed login. First, there will be no error message on the login screen indicating an authentication failure and second, there will be a new icon in the lower right-hand corner indicating that cookies have been blocked.

In such a case, you can do one of the following:

- Add the second (and subsequent) Control Station with a fully-qualified hostname that indicates that the system is in the local intranet.
- Add the IP address to the list of trusted sites.
- Double-click the blocked cookie icon. From the resulting dialog box, a user can indicate that cookies should be accepted from that site in the future.

Internet Explorer for Windows Server 2003

Windows Server 2003 has a feature known as *Internet Explorer Enhanced Security Configuration,* which is enabled by default. This effectively means that you cannot use a Windows Server 2003 client system to reach Unisphere without making changes to the default configuration. One of the biggest changes that Windows Server 2003 security configuration brings about is that all Internet and local intranet sites are assigned to the Internet zone, which has a security level of High by default. This prevents scripts and Java applets from properly loading and running.

If appropriate[2], the best solution is to place the Celerra Control Station into the local intranet zone. Unlike in other versions of Windows, you must do this explicitly in Windows Server 2003. No systems are automatically added to the local intranet zone. It is not sufficient to simply add the Control Station to the list of trusted sites. This will not enable the full set of scripting and applets features that are required.

This feature is explained in Microsoft Knowledge Base Article 815141, *Internet Explorer Enhanced Security Configuration Changes the Browsing Experience*, and may be viewed at Microsoft's website.

Troubleshooting

Browser reports a "Hostname Mismatch" with the SSL certificate

There are several reasons that a browser might display dialog box reporting issues with the SSL certificate from the Control Station. Most of these circumstances are related to the initial installation and setup of the Control Station.

---

[2] This would be appropriate if the Control Station actually resides in your local intranet zone.

Repeated dialog boxes

When you first point your Web browser to a Control Station, there may be several dialog boxes asking about SSL certificate issues. However, if the Control Station's self-signed SSL certificate is installed in both the Web browser of choice and the JRE, then this should be a one-time event. In addition, if you use the fully-qualified domain name to point your browser at the Control Station, you will not get `Hostname Mismatch` warnings.

Unisphere does not display issues

Ensure that you select the certificate option to **Always trust content from this publisher** or **Permanently store this exception**. If you do not select these options, the Unisphere management screens will not appear. Instead, you may see just a blue screen. The screens will not load due to the invalid certificate.

Deleting cookies from the browser

If you delete stored cookies, you may find that your access to Unisphere and Celerra Monitor has been affected. The remedy is to log in again.

Conclusion

This white paper explained how Unisphere can be affected by the user's browser settings for security and privacy. It described how the Celerra Control Station:

- Manages SSL certificates
- Uses cookies and session tokens

References

- Microsoft Knowledge Base Article 815141: *Internet Explorer Enhanced Security Configuration Changes the Browsing Experience*
- Microsoft Knowledge Base Article 283185: *How to Manage Cookies in Internet Explorer 6*