Report # C4-58R-02

Guide to Securing Netscape Navigator 7.0

The Network Applications Team
of the
Systems and Network Attack Center (SNAC)

Author:
Curt Doernberg

Updated: December 2002
Version 1.0

SNAC.Guides@nsa.gov

This page intentionally left blank.

Warnings

- **Do not attempt to implement any of the settings in this guide without first testing in a non-operational environment.**
- Many of the security related issues associated with Netscape are interrelated. The reader is encouraged to gain familiarity with the entire document before implementing the recommendations in this guide.
- This document is only a guide containing recommended security settings. It is not meant to replace well-structured policy or sound judgment. Furthermore, this guide does not address site-specific configuration issues. Care must be taken when implementing this guide to address local operational and policy concerns.
- SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED. IN NO EVENT SHALL THE CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
- This document is current as of the date listed on the cover page. Please keep track of the latest security patches and advisories on the Netscape Security Center at http://wp.netscape.com/security/index.html. Also, please read the release notes that come with Netscape Navigator.

Trademark Information

Table of Contents

Table of Figures

Chapter 1: Introduction

Intended Audience

This document is intended for an Administrator of a Windows network supporting users running Netscape Navigator 7.0. This document can also be used for a standalone machine running Netscape on Windows, although the owner of this machine would be responsible for both administrative and user responsibilities mentioned in this document. This document may provide insight for both users of Netscape Navigator 7.0 on non-Windows platforms and users of similar versions of Mozilla on any platform, however this guide was not developed with these environments in mind.

Notation

The term Netscape has at times referred both to Netscape Communications Corporation and its products including a web browser, a web server, and other products. In this document, the unadorned term Netscape is used exclusively to refer to Netscape Navigator 7.0, the current web browser product distributed by Netscape Communications Corporation.

All Netscape preferences can be found by selecting the Preferences item from the Edit menu. In this document's notation, the first colon-delimited field is the primary entry in the category section, and successive fields (if any) either refer to secondary entries in the category section or sections of the right side panel for that setting. An example of this notation is:

Privacy & Security:Master Passwords:Master Password Timeout (shown in Figure 1)

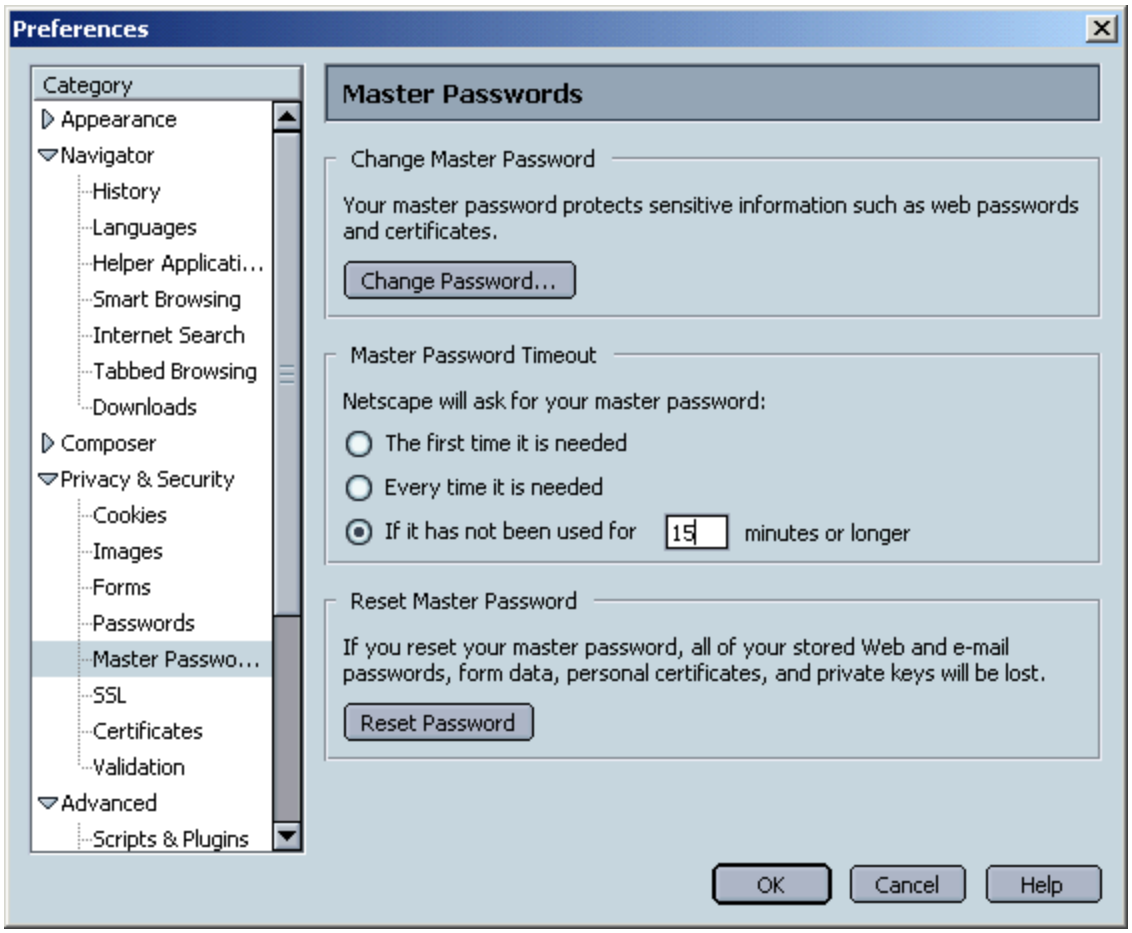

Figure 1 - Privacy & Security:Master Passwords

Implementation

The simplest way to implement this configuration guidance is to install and configure Netscape as per this document on all the machines and templates that will include Netscape. In cases where Netscape is preinstalled and implementing this guidance is desired without touching every machine or template, and in cases where configuration is to be reapplied periodically, a sample VBS script to modify the user's preferences file is provided in Appendix C. The script implements many but not all of the recommendations in Chapters 3 through 5, and can be customized. Those settings that cannot be automatically set via script will be so noted throughout the document. The sample script can be used as a logon script through Windows 2000 Group Policy. While it may be possible to use this script as part of a Windows NT logon script, such a task would require a knowledgeable NT administrator and is beyond the scope of this document.

Chapter 2: Installation Options

The following options are recommended for installation of Netscape. For those options where “no opinion” is stated, they were disabled in the configuration used when creating this guide; however, the decision to install these options should be based on local policy. It should be noted that some of these options relate to separate products that require their own security maintenance. Refer to the vendors’ web sites for the latest information.

These settings are not controllable by logon script; therefore Netscape must be installed with these options set correctly on each computer or computer template.

Custom Installation

Navigator – checked

Mail and Instant Messaging – unchecked

One peculiar aspect of the Netscape 7 distribution is that the installation of Mail & News support has been linked to the installation of two Instant Messaging systems: AOL Instant Messenger and ICQ. Mail & News support is seen as a feature appropriate for use on enterprise networks, while Instant Messaging is seen as inappropriate in many organizations. Because of the combination of an appropriate feature and an inappropriate feature in this installation option, enabling this installation option is not recommended.

Spell Checker – no opinion

Sun Java 2 – checked

More information about Java is in Appendix A

Quality Feedback Agent – unchecked

Crash information has the potential of including the information in the web browser at the time of the crash.

AOL ART Extensions – no opinion

Net2Phone – unchecked

This guide makes no recommendation on the subject of Internet Telephony such as Net2Phone. However, the decision to use such software warrants a separate policy decision. For this reason, Net2Phone is recommended at unchecked as a part of the Netscape installation.

Macromedia Flash Player – no opinion

RealPlayer8 – no opinion

Viewpoint Media Player – no opinion

Winamp – no opinion

HP Printer Identifier Plugin – no opinion

Classic Skin – no opinion

Canadian region pack – no opinion

Program Folder – Netscape 7.0

Quick Launch – checked

Netscape.com home page – no opinion

Chapter 3: Secure Web Server Connections

Netscape offers the ability to create a secure connection to a web server. This secure connection is supposed to provide two guarantees to the user – the web server is the authentic web server for this address (traditionally termed authentication), and there is no possibility of communications being viewed or modified in transit (traditionally termed confidentiality and integrity). The theme of settings in this section is to help bolster Netscape's support of these guarantees.

It is also important to understand two things that Netscape will not do for you. First, when Netscape is not providing a secure connection (as noted by the unlocked lock icon), these two guarantees of a secure connection do not apply. It is the user's responsibility to ensure that a secure connection exists before either transmitting or receiving information for which these guarantees are required. Second, a secure connection protects the data in transit, not at rest. It is up to the owners of the web site to protect and properly use the data once it comes into their possession, and it is up to the user to communicate sensitive data only to web sites that they trust with their data.

Privacy & Security:Certificates:Manage Certificates

By clicking on Manage Certificates, you see the Certificate Manager window, shown in Figure 2, where stored user certificates and trusted root certificates are shown. Make sure that certificates in the trusted root store match relevant policy as to which certificates should be trusted. For example, if an organization has in its policy to support the DoD PKI, the DoD PKI root certificate(s) should be installed.

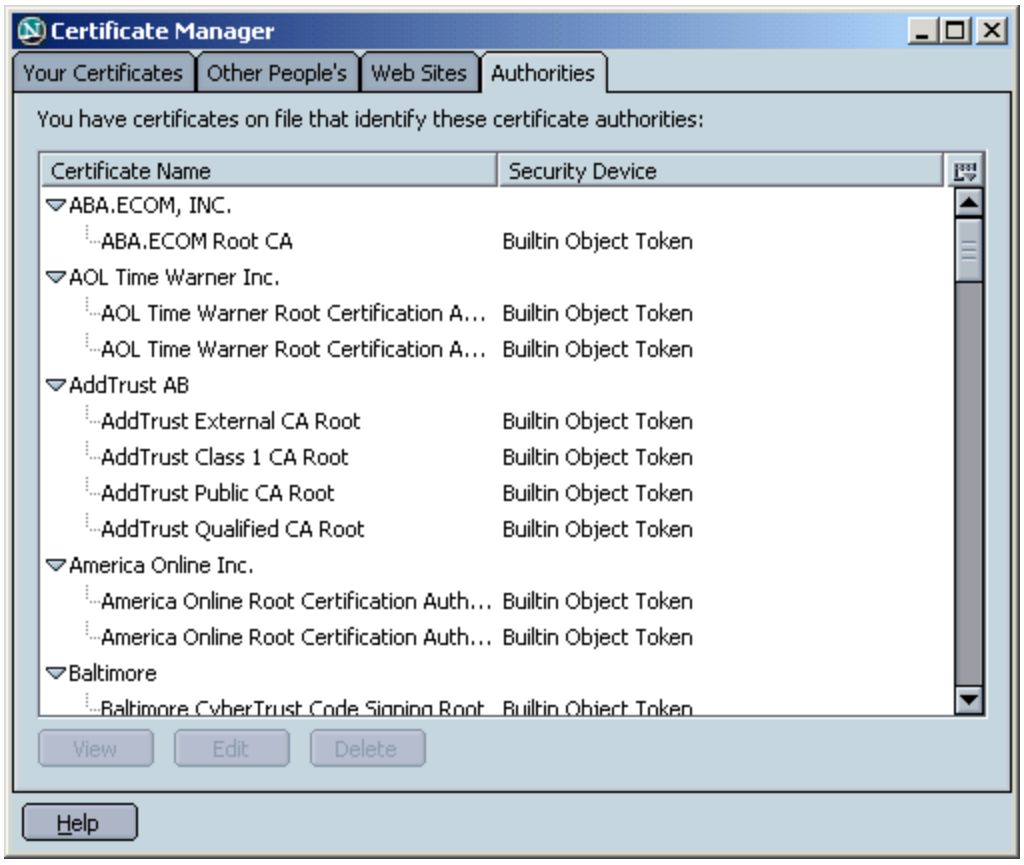

Figure 2 - Certificate Manager

Certificates can be installed by opening the .cer file with Netscape. When doing this, you receive the following dialog (Figure 3):

Figure 3 - Downloading Certificate

In the “Downloading Certificate” dialog you should approve those certificate use purposes for which you trust the certificate. You should click the view button to pull up the Certificate Viewer (Figure 4) and confirm that the SHA1 and/or MD5 fingerprints match those of the certificate as derived from another source (most often a publication for a widely used certificate, or a phone call for a sparsely used certificate).

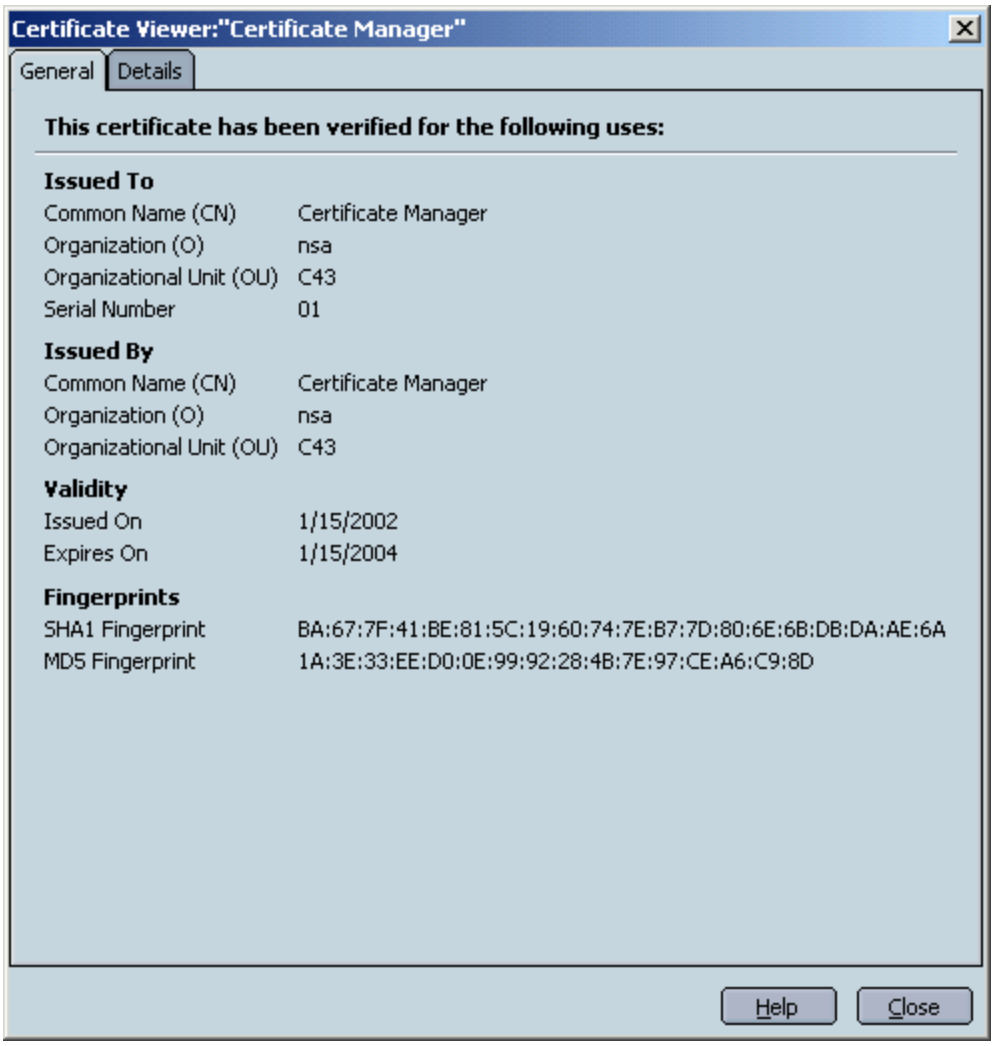

Figure 4 - Certificate Manager

Privacy & Security:Certificates:Manage Security Devices

This setting allows you to add additional security modules. This would most likely be used with a smart card or other security hardware device. If you are not using special hardware and do not have any special need for custom security modules, then no changes need to be made here. For reference, the default state of this window is found in Figure 5.

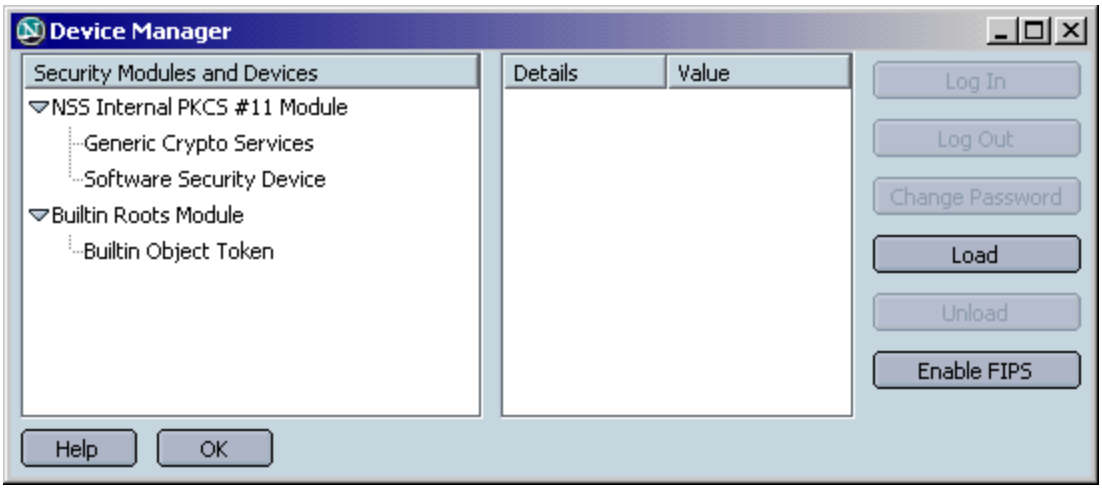

Figure 5 - Privacy & Security:Certificates:Manage Security Devices

Privacy & Security:Validation

One fundamental component of certificate-based trust is that the Certification Authority (CA) must have a method for revoking that certificate. The two methods supported by Netscape are Certification Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP). For each CA trusted in the certificate store, Netscape should be configured with at least one method of verifying that a certificate issued by that CA has not been revoked.

Failure of web browsers and CAs to coordinate on automated methods for checking revocation continues to be a security weakness at the time of this writing. Therefore, it may not be possible to specify a validation source for each CA preinstalled with Netscape. This should factor into the policy decision as to which CAs are kept in Netscape's "Authorities" certificate store.

Privacy & Security:Validation:OCSP

The OCSP setting should be set to "Use OCSP to validate only certificates that specify an OCSP service URL".

OCSP is a method that a client can use to verify that a certificate has not been revoked. Certificate Authorities that provide OCSP service will include a URL inside these certificates.

It is possible that an internal or external service could be used to track all invalid certificates by combining information from several CRLs and/or OCSP servers. If such a service is available and appropriate for your network, then the option "Use OCSP to validate all certificates using this URL and signer" should be selected and its information should be filled out as appropriate for this service.

The option "Do not use OCSP for certificate validation" should never be enabled. OCSP validation requires the same network connectivity to access the OCSP server as it does for the certificate that requires it. Therefore, if you can reach the web server that has the certificate, you should also be able to reach the OCSP server to check that certificate's validity. Exceptions to this are most likely a result of limitations imposed by the local firewall or proxy server.

The only setting supported in the configuration script provided is the initial recommendation.

Privacy & Security:Validation:CRL

For those CAs that do not support OCSP, CRLs should be installed into Netscape. The procedure for doing this is to browse in Netscape to the CRL location (such as http://crl.verisign.com) and click on the CRL to be installed. You should see a prompt like Figure 6.

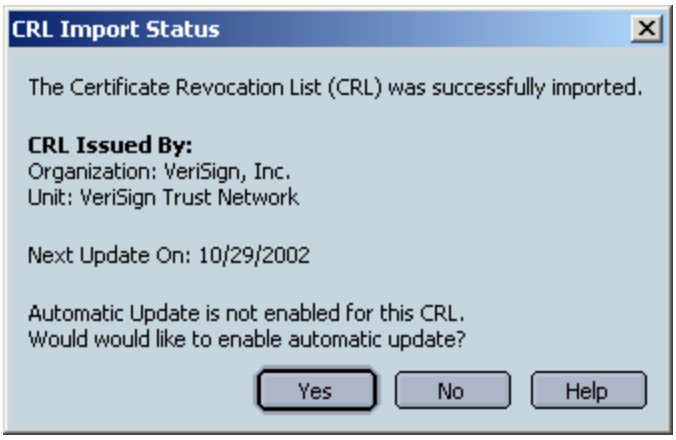

Figure 6 - CRL Import Part 1

Select yes to enable automatic update. Unless you are operating under a policy that specifies these values, the default options to "Enable Automatic Update for this CRL" and "Update 1 Day(s) before Next Update date" (as shown in Figure 7) will get CRL information at a reasonable rate.

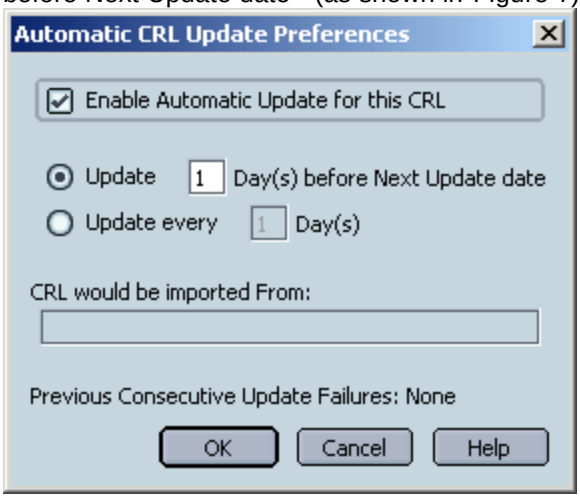

Figure 7 - CRL Import Part 2

Repeat this procedure (starting from browsing to a CRL location) as needed for each CA and all of a CA's CRLs, keeping in mind that a given company might have several CAs and/or CRLs.

This procedure is not performed in the configuration script.

Privacy & Security:Certificates:Client Certificate Selection

In most cases, this should be set at "Ask Every Time". Use of a client certificate is usually uncommon enough that the user should be aware of each use.

Advanced:Proxies

This setting does not perfectly fit into this chapter, because use of secure connections for important web pages should prevent exploits that rely on a malicious proxy. However, to protect against malicious proxy exploits for ordinary http requests, it is important to ensure that Netscape's proxy settings are set correctly for your network (the correct settings will depend on how your proxy server is set up).

WARNING: Mistakes in the proxy settings will cause web browsers to fail until the settings are corrected. For this reason, implementation in the provided script must be uncommented before it will be active.

Privacy & Security:SSL

The SSL Protocol Versions should be set as follows:

- Enable SSL version 2 – unchecked
- Enable SSL version 3 – checked
- Enable TLS – checked

SSL Warnings should be set as follows:

- Loading a page that supports encryption – unchecked

  This warning is generated to alert the user that an SSL session is about to begin. The threat is lack of SSL when it is needed, and the precaution for this threat is for the user to actively check the lock icon (looking for secure  as opposed to the typical insecure ) at the time of information submission. This is generally considered preferable to the user receiving a plethora of alert boxes that will quickly become ignored.

- Loading a page that supports low-grade encryption – checked

  If the guidance in this chapter is followed to disable weak encryption protocols and cipher suites, this warning should never appear. If low-grade encryption is allowed, then this will warn the user when it is in use.

- Leaving a page that supports encryption – checked

  This will remind the user when a secure session is ending, as well as alert the user if Netscape is alternating between secure communications and insecure communications.

- Sending form data from an unencrypted page to an unencrypted page – checked

  This warning is useful because it allows the user an opportunity to reconsider if form data contains information of sufficient sensitivity to require a secure connection. If the user feels that submitting data in the clear is appropriate even after a warning, then Netscape will allow it.

- Viewing a page with an encrypted/unencrypted mix – checked

  The information contained in this warning also shows up in the lock icon as follows (). This means that only part of the page is encrypted, and part of the page is not. The reason that this warning should be enabled is because the situation is sufficiently unusual that users do not necessarily recognize the broken lock icon.

Further, as found by clicking Edit Ciphers, the Ciphersuites should be set as follows (Figure 8):

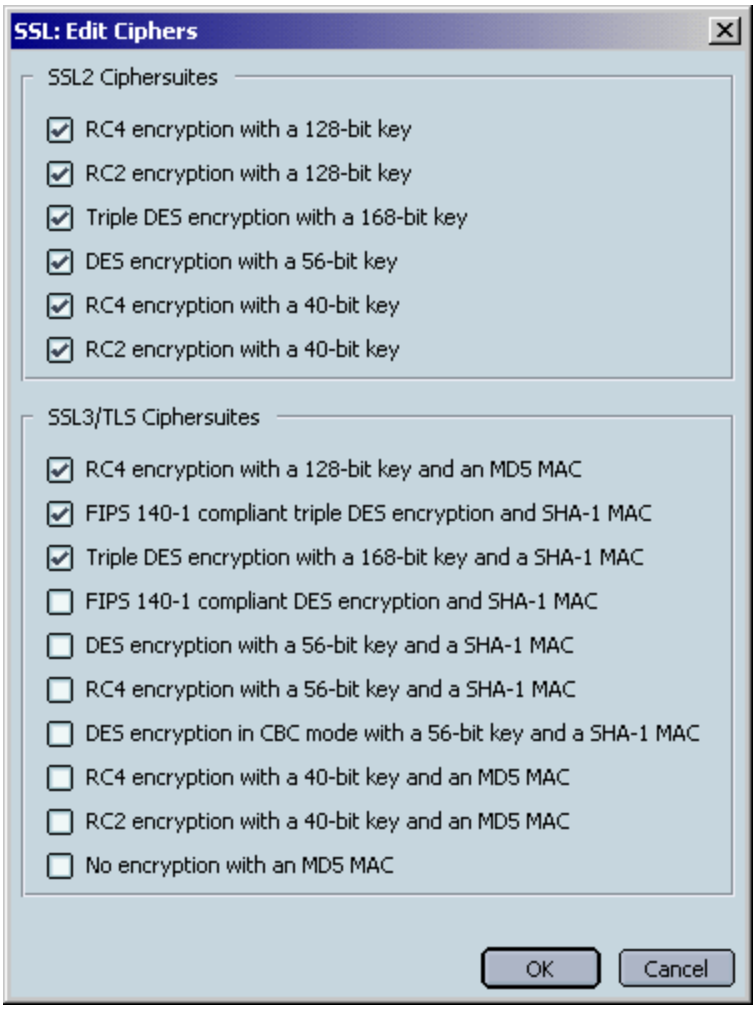

Figure 8 - Edit Ciphers

For the SSL2 Ciphersuites

- All Ciphersuites – checked (If disabling SSL2, these are irrelevant. If SSL2 is enabled because of the warning below, then all SSL2 Ciphersuites should be available for compatibility.)

For the SSL3/TLS Ciphersuites:

- RC4 encryption with a 128-bit key and an MD5 MAC – checked
- FIPS 140-1 compliant triple DES encryption and a SHA-1 MAC – checked
- Triple DES encryption with a 168-bit key and a SHA-1 MAC – checked
- All other SSL3/TLS Ciphersuites – unchecked

WARNING: There are some web servers that do not support encryption that previously required a US export license, and will thus be unable to negotiate a secure link with a web browser that follows these recommendations. If compatibility with these web servers is more important than using good cryptography for all secure connections, then consider the following two changes.

1. Modify SSL3/TLS Ciphersuites to enable those Ciphersuites based on DES. While this only provides 56 bits of encryption, this is sufficient for some purposes. This will add some compatibility at the expense of some security.
2. Allow the SSL2 protocol to be used, along with all Ciphersuites that it supports. This will add more compatibility at the expense of more security, because SSL2 has known security problems.

Chapter 4: Executable Content

Netscape interprets much more than HTML. It is common to see web pages that include images, scripting, embedded objects, and many other features. The possibility exists that some object or code that is part of a web page could cause malicious code from that website to run on the local machine. The theme of settings in this section is limiting the types of objects and code that Netscape can view to those that do not provide such an automated entry for malicious code.

It is important to understand what Netscape will not do in terms of preventing Executable Content threats. The best-configured Netscape will not stop you from going to a website, downloading an executable containing a virus, and running that executable (other security measures, such as virus protection software and least privilege user accounts will reduce exposure to this threat, but might not eliminate it). While Netscape should prevent automatic execution of malicious code, it is the user's responsibility to only manually run those mobile code types allowed by policy.

Navigator:Helper Applications:Plug-in Finder Service

The option "Always use the Netscape Plug-in Finder Service (PFS) to get plug-ins" should be checked.

Plug-ins are additional applications that allow Netscape to display data of formats it cannot display itself, such as Acrobat, Flash, RealPlayer, and various others. This option only matters when Netscape is presented with a page including a type of file it does not already possess a plug-in for.

If this option is checked, Netscape will query a CGI script at netscape.com for a URL to an installer for a plug-in that will handle the new type. If this option is unchecked, then the plug-in can be downloaded with user confirmation from a URL specified by the owner of the web page (although the netscape.com CGI script will be used if this field is not specified).

Neither of these options is a desirable state of affairs; automatic installation is something that was mentioned in the introduction to this section as something to avoid. It is preferable that acceptable plug-in applications be selected and installed by the Administrator in advance, and that users not have the ability to install additional applications. However, if forced to select someone to provide automatic plug-in installation over the Internet, Netscape Communication Corporation should be trusted as the authority on which applications are safe for use with their browser.

Navigator:Downloads

The option "When starting a download" should be set to "Open a progress dialog" or "Open the download manager". Do not set this option to "Don't open anything".

This setting determines what should appear to the user when a file download is begun. While this setting seems to have marginal security significance, the possibility of files silently being downloaded is sufficiently undesirable that the "Don't open anything" option should not be selected.

Advanced:Enable Features That Help Interpret Web Pages

The "Enable Java" option (shown in Figure 9) should be checked. Java has a good security model for which actions are appropriate for mobile code. It is implemented in a way that unsafe actions are only allowed if the policy approves them. The default policy appears to allow unsafe actions only to applets with a valid certificate. For this reason, Java is considered safe enough to run code provided by an untrusted website. More information about Java can be found in Appendix A.

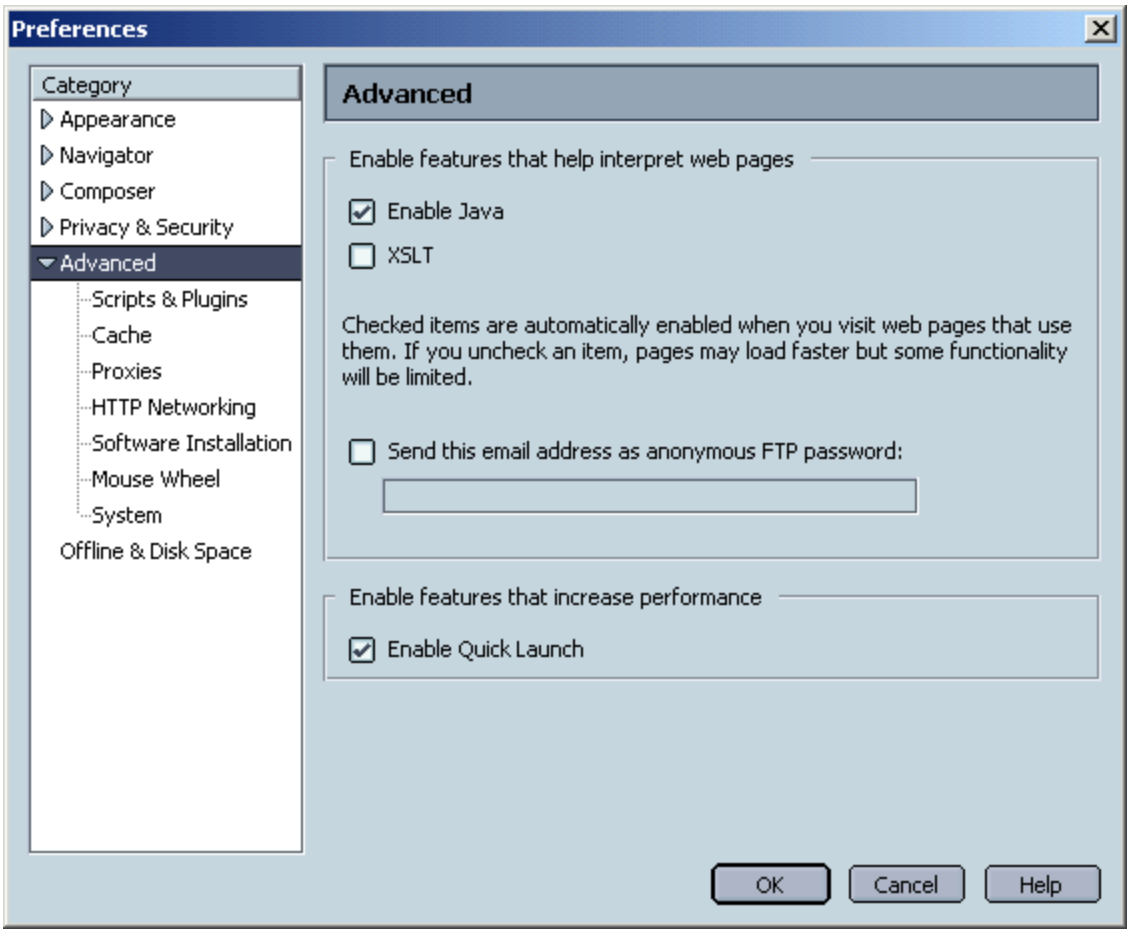

Figure 9 - Advanced

The XSLT option (also shown in Figure 9) should be unchecked. XSLT is a standard language used for transforming XML documents into other formats including HTML and alternate XML. Because it is a new language, it is likely that the security models for both the language and Netscape's implementation of the language have not yet been thoroughly tested, therefore, it should be turned off.

WARNING: When presented with a page that expects to use XSLT, and XSLT is disabled, Netscape may either display a blank page or display the raw XML. XSLT is only used sparsely at the time of this writing, so this does not appear to be a significant problem. If inability to display XSLT is a problem for your users, consider either recommending that they enable XSLT on a per page basis or changing the XSLT setting to checked.

Advanced:Scripts & Plugins

The "Enable JavaScript for Navigator" option should be checked. Netscape's implementation of JavaScript is designed to limit functionality to that appropriate for use by a web page. Many web pages use JavaScript in ways that enhance the user's web browsing without posing any additional security risk. While there have occasionally been flaws in JavaScript implementations, and while web sites continue to have Cross-Site-Scripting vulnerabilities, overall JavaScript provides more benefit than it adds risk for most environments.

Although Mail and News are not recommended as part of this configuration guide, if Mail and News are installed, the option "Enable JavaScript for Mail and News" should be unchecked. This is because it is easier to push a malicious mail message to a user's inbox (as many e-mail worms have demonstrated) than it is to pull users to a malicious web page.

Advanced:Scripts & Plugins:Allow Webpages To:

This group of settings allows you to disable the features of JavaScript considered most easily abused. These features, along with recommendations are summarized in Table 1:

Table 1 - JavaScript Features

Feature Name	Feature Recommendation
Open a link in a new window	Enabled
Move or resize existing windows	Enabled
Raise or lower windows	Enabled
Hide the status bar	Disabled
Change the status bar text	Disabled
Change images	Enabled
Create or change cookies	Disabled or Enabled
Read cookies	Disabled or Enabled

The “Hide the status bar” and “Change the status bar text” options allows scripts to override Netscape’s use of the status bar with their own. Netscape typically uses the status bar to display the URL associated with a link that the user has their mouse over. This can be used to display accurate human-readable text, such as displaying “The United States Navy” for a link to www.navy.mil. However, it could also be used to obscure a malicious URL, where such a malicious URL could point to the wrong server (PayPa1 instead of PayPal) or contain an attack (such as Unicode or XSS (cross-site-scripting)). These two options should, therefore, be disabled.

The “Read cookies” and “Create or change cookies” options deal with the ability to read and write cookies from a script. These options allow restrictions above and beyond those in the section Privacy & Security:Cookies. One reason to consider using these options is for protection from XSS attacks. Although it is the web server’s responsibility to prevent XSS attacks from reaching Netscape, some web servers still have vulnerabilities of this type. On the other hand, setting cookies from a script can be a completely legitimate behavior, and thus disabling these options will break websites that rely on this behavior. The “Read cookies” and “Create or change cookies” options should be disabled if preventing XSS attacks is more important than allowing this type of legitimate cookie use, otherwise it should be enabled.

The options not explained do not appear to have security implications, though some may be disabled to reduce JavaScript’s use in displaying extraneous content. This may also prevent some legitimate content from displaying as well.

Advanced:Software Installation:Manage Software Installations and Updates

The “Enable software installation” option should be unchecked for everyone on an enterprise network, although for different reasons.

For typical users, they should not have permission to install the updates, so enabling software installation only allows the user to see a later and more confusing error message.

For Administrators, allowing them to install updates automatically may remove some of the impetus to go through proper procedure to download, verify, and install new software and software updates throughout their network rather than just on their own machines.

On a self-administered system, the “Enable software installation” option can be checked if the update mechanism specified in the relevant policy is automatic updates.

Advanced:Software Installations:Update Notifications

For typical users, “Check for updates:” should be unchecked. As mentioned above, a typical user should not have the ability to install an update, and therefore giving them notice that an update is available is not useful.

Administrators should have the “Check for updates:” option enabled and set to weekly. This will remind them when it is time to update Netscape, and hopefully cause them to update Netscape throughout the rest of the network.

On a self-administered system, the “Check for updates:” option should be enabled and set to weekly.

By default the provided script disables automatic update checking for all users.

Chapter 5: Stored Information

This section deals with security settings involving ways Netscape stores information about its users, about its users' behaviors, and the web pages that its users have seen. The most prominent of these methods is the use of cookies, which can be used to track a users' activity on the web. The theme of the recommended settings is to either reduce information stored by Netscape or make this information harder to access without user approval.

These settings only limit the information that Netscape automatically provides to websites. No setting can prevent a user from manually providing more information than appropriate to a website. Websites can and do record user activity even without the help of Netscape supported features, such as cookies, so it is important to only send sensitive information to a website you trust to use that information properly.

Privacy & Security:Cookies

This page controls how Netscape deals with cookies. As shown in Figure 10, this setting should be set at "Enable cookies based on privacy settings". Both the "Ask me before storing a cookie" and the "Limit maximum lifetime of cookies to:" options can remain unchecked.

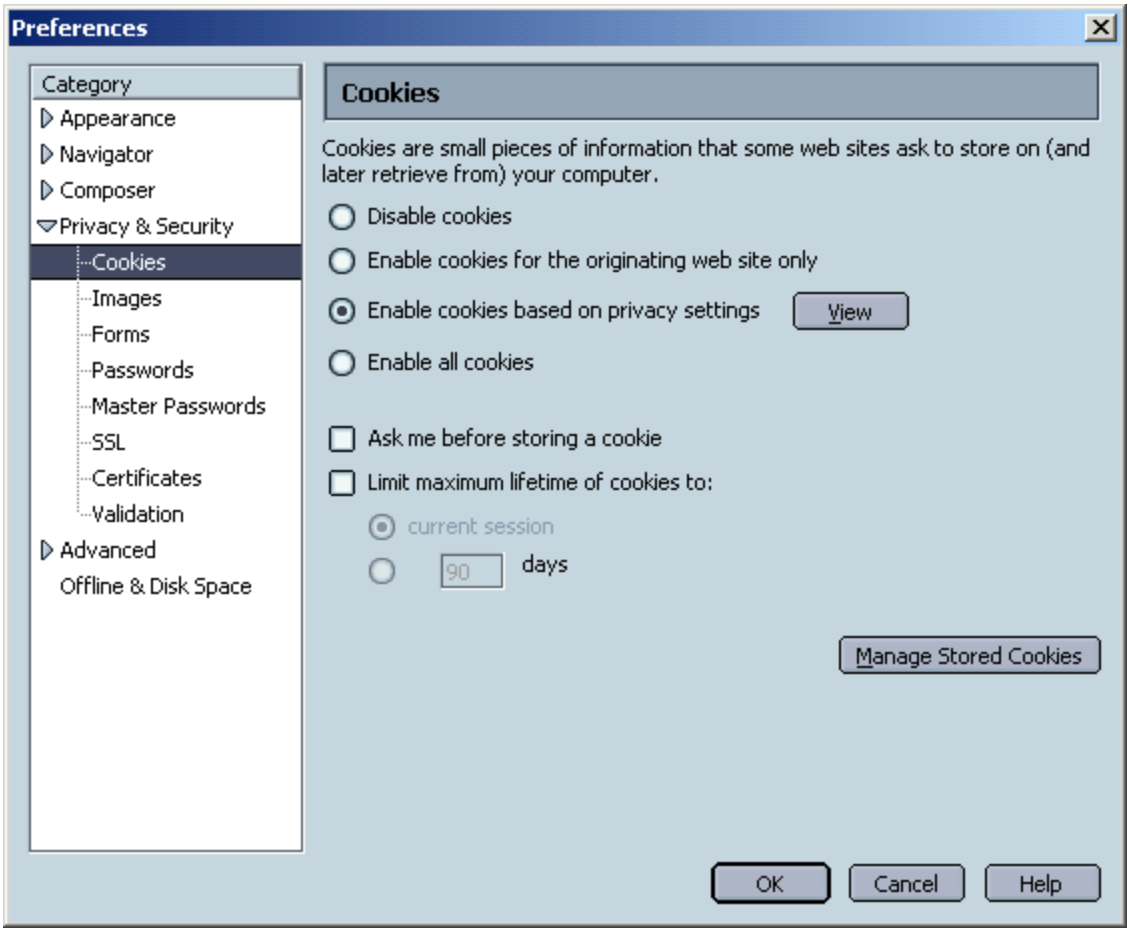

Figure 10 - Privacy & Security:Cookies

The “Ask me before storing a cookie” option should be unchecked because normal web browsing will encounter too many cookies for the user to want to see a prompt for each cookie.

The “Limit maximum lifetime of cookies to” option should be unchecked because there is no added security risk associated with cookies persisting on the hard drive, and there is a positive convenience factor for not having to recreate website-specific preferences.

Further, select “View” and select the predefined Level of Privacy called high, as shown in Figure 11.

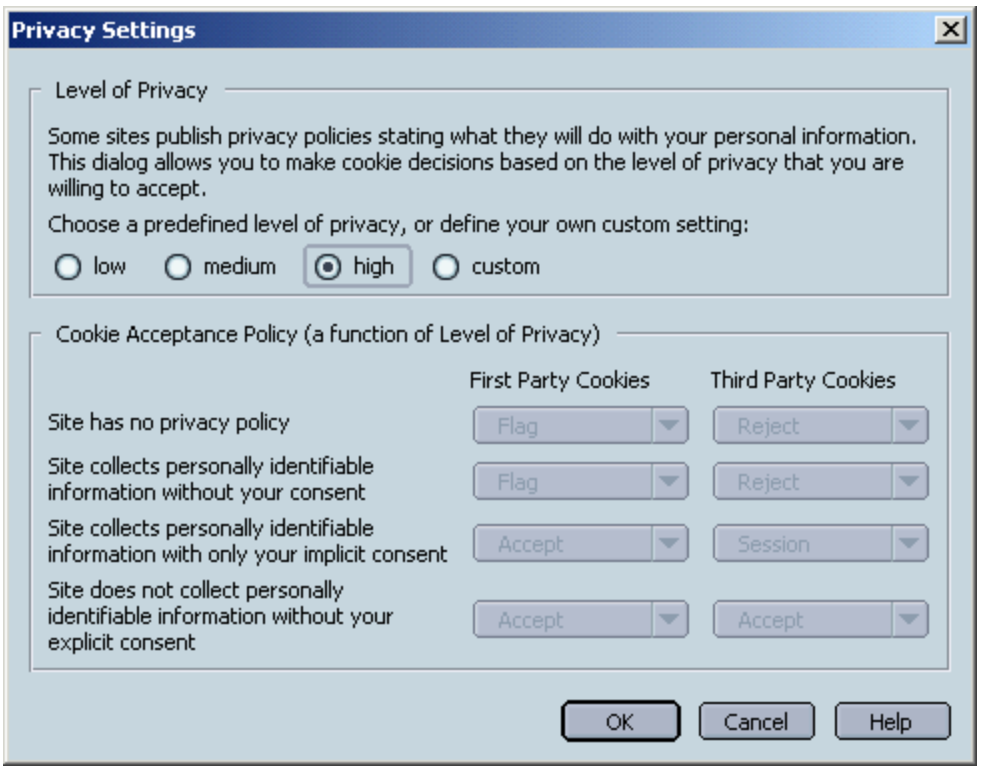

Figure 11 - Privacy Settings

The Platform for Privacy Preferences (P3P) standard for privacy settings specifies that a summary of how the cookie will be used should be sent with each cookie in order to allow web browsers to automatically accept or reject cookies based on a policy. Although many web sites do not yet support P3P, this feature degrades gracefully by having good settings for the category “Site has no privacy policy”. The High privacy level will cause a little eye ( ) to appear in the bottom right corner to warn you about a first party cookie with either no P3P policy or an unacceptable P3P policy. This privacy level will also block third party cookies with either no P3P policy or an unacceptable P3P policy.

If local policy specifies handling of cookies, or if you have interest in customizing these settings, the recommended mechanism is through the use of a custom value for the Cookie Acceptance Policy. One reason for such an interest is to make a different tradeoff between functionality and privacy/anonymity. The help button in Figure 11 will provide some useful information, as will the P3P website cited in Appendix B: Netscape Security References. Note that extreme policies that do not rely on P3P, such as treating all cookies as session cookies or rejecting all cookies, could also be implemented using this mechanism.

The script currently sets cookie behavior to P3P with the predefined high privacy level. An example of a custom P3P Cookie Acceptance Policy, along with additional information, is available within the sample script. The easiest way to implement your own custom policy via script is to set the desired Cookie Acceptance Policy on one machine, read the resulting value for “network.cookie.p3p” from your prefs.js file, and insert that value into the script as a custom privacy level.

Privacy & Security:Form Manager

The option “Save form data from web pages when completing forms” should be unchecked. When checked, and the user fills out a form, Netscape will prompt the user to store the form’s data for use in automatically filling out other forms. When unchecked, the user must actively go to the “save form info” or “edit form info” menu items under the form manager submenu of the tools menu.

Netscape can store information of various sensitivity, along a spectrum from information that could be found in a phone book to credit card information to information often used as authentication (including social security number and mother’s maiden name). It is preferable that users that wish to take advantage of this feature be forced to actively store information that they feel appropriate in Netscape rather than reactively click OK to a prompt. While theft of stored data does not appear to be a current threat, it is possible that a flaw would allow a malicious website to automatically extract data stored here.

Privacy & Security:Passwords:Password Manager

The “Remember passwords” option can be checked or unchecked according to policy. In formulating a policy about storing passwords, the following conflicting ideas should be considered:

- If users have too many passwords to remember, then they are more likely to write them down, pick bad passwords, or reuse the same passwords in different places.
- If Netscape knows a password, a possibility (though hopefully a very small one) exists that Netscape could be exploited in such a way that it would use this password without the user’s authorization. This risk seems to be partially mitigated through use of Master Password features (see the next three settings).

A good balance between these considerations is that users should allow Netscape to remember passwords only for lower sensitivity websites, and that users remember unique passwords for web sites of higher sensitivity. Determining which level of sensitivity deserves which treatment can be a matter of policy or can be left to the discretion of users.

By default, this script leaves use of this feature to the user. Code under the “Remember Passwords Using the Password Manager” section can be uncommented in order to force this feature to be disabled.

WARNING: There is an important dependency between the settings on this page. In order for Netscape to require the user to enter the Master Password as a control factor on Netscape's access to stored data (the Master Password Timeout setting), the "Use encryption when storing sensitive data" option must be checked AND a non-blank Master Password must be set.

Privacy & Security:Passwords:Encrypting versus Obscuring

The "Use encryption when storing sensitive data." option should be checked.

Although human beings cannot necessarily read passwords out of Netscape's data files, a program designed for this purpose can. By checking this option, it is no longer possible for such a program to automatically translate data files into usernames and passwords. This option provides protection for passwords at rest, and has no effect on Netscape's ability to use passwords in the current user's profile.

Privacy & Security:Master Passwords

Each user should set their Master Password to a non-blank password according to relevant guidance on selecting good passwords. Good passwords have length (minimum 8 characters, but 12 or more is preferable) and contain letters (upper and lower case), numbers, and other characters such as punctuation.

Selecting a Master Password will cause Netscape to request the Master Password before using any protected information. As per documentation, this information includes the following items:

- Web passwords
- e-mail passwords
- stored form data
- personal certificates
- private keys

Note that Master Passwords cannot be set by script, users must manually create their own passwords.

Privacy & Security:Master Passwords:Master Password Timeout

This should be set at "If it has not been used for X minutes or longer", where X is a relatively short time interval such as 15 minutes.

As noted above, once a Master Password is chosen, its input is required before Netscape will retrieve certain types of stored personal information. This setting determines how frequently the Master Password must be input. The setting "The first time it is needed" is not often enough, because a user that allowed the use of protected information shortly after starting Netscape does not necessarily want protected information available to a cross-site-scripting attack later in the day. The setting "Every time it is needed" has the potential to become too cumbersome.

Appendix A: Java Runtime Environment

Netscape includes the 1.4.0_01 J2SE (Jave 2 Standard Edition) JRE (Java Runtime Environment) from Sun Microsystems. The JRE is responsible for the security of Java Applets, including Security Monitor verification that behavior is appropriate to policy, as well as verifying digital signatures associated with additional privileges. This software can be updated from http://java.sun.com by getting the latest JRE for your platform. Updated JREs typically include bugfixes, some of which address security concerns.

The certificate store used by the Java Plug-in is different than the one used by Netscape. Its default location is C:\Program Files\Java\j2re1.4.0\lib\security\cacerts. Future implementations of Java and Netscape may include certificate verification and may allow for better integration of these two certificate stores.

As discussed in the beginning of Chapter 3, it is important that the certificates in this keystore correspond to those organizations trusted by policy to sign code-signing certificates. Full documentation about keytool is available from Sun (http://java.sun.com/j2se/1.4.1/docs/tooldocs/windows/keytool.html), however this paper will include brief demonstrations of how to view, add, and remove keys from the default keystore.

As illustrated in Figure 12, by setting the path to include the Java bin directory, changing into the directory containing the cacerts and running the following command, all CAs used by Java will be listed.

```
keytool –list –keystore cacerts
```

More detailed reports can be generated by adding the –v option to the previous command.

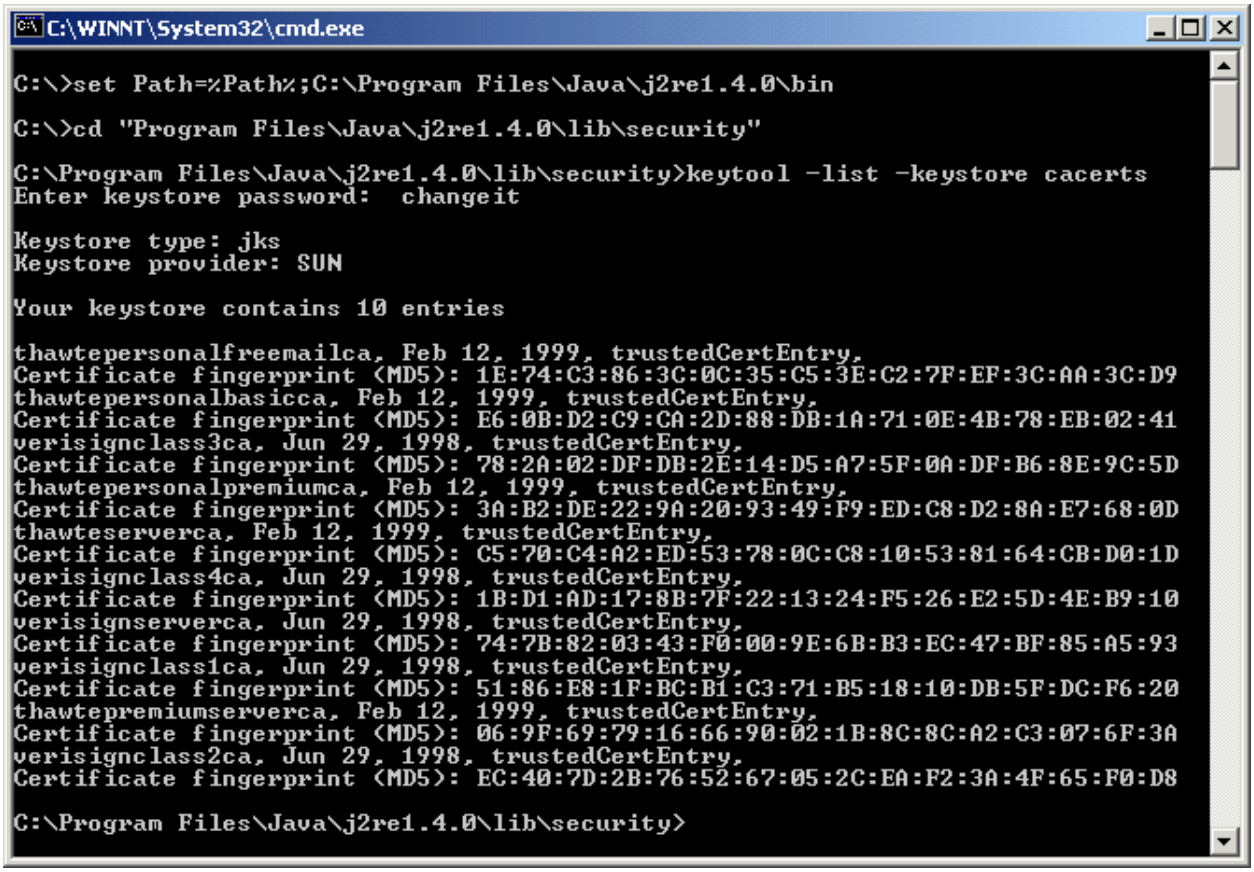

Figure 12 - Listing Certificates

Your policy should determine what certificates should remain in the trusted CAs store. In order to implement this policy, examples of adding and removing a certificate are provided below. **These examples are for illustration only and are not recommended for implementation exactly as shown.** Both of these examples assume that the PATH has been set to include the java bin directory.

As illustrated in Figure 13, by running the following command, the CA specified by <Alias name> will be deleted.

```
keytool –delete –alias <Alias name> -keystore cacerts
```

This is how you remove any CAs that are installed by default but are not trusted by your policy.

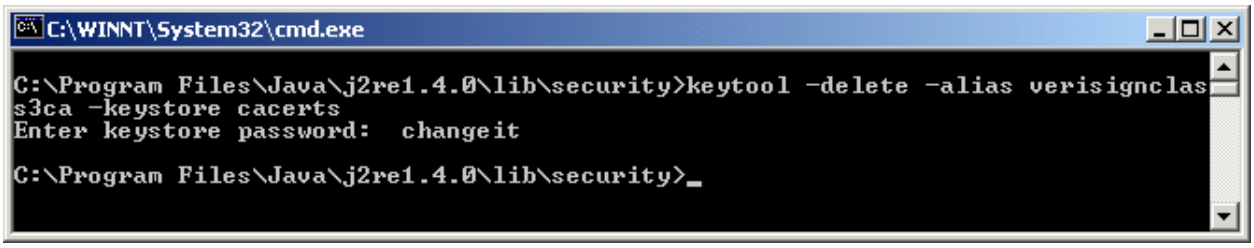

Figure 13 - Deleting A Certificate

As illustrated in Figure 14, by running the following command, a new CA whose file is specified by <CertFileName> is imported into the CA's store.

```
keytool –import –trustcacerts –alias <Alias Name> -file <CertFileName>
```

Notice that keytool requires you to read the certificate information and fingerprints and type yes in order to accept the certificate.

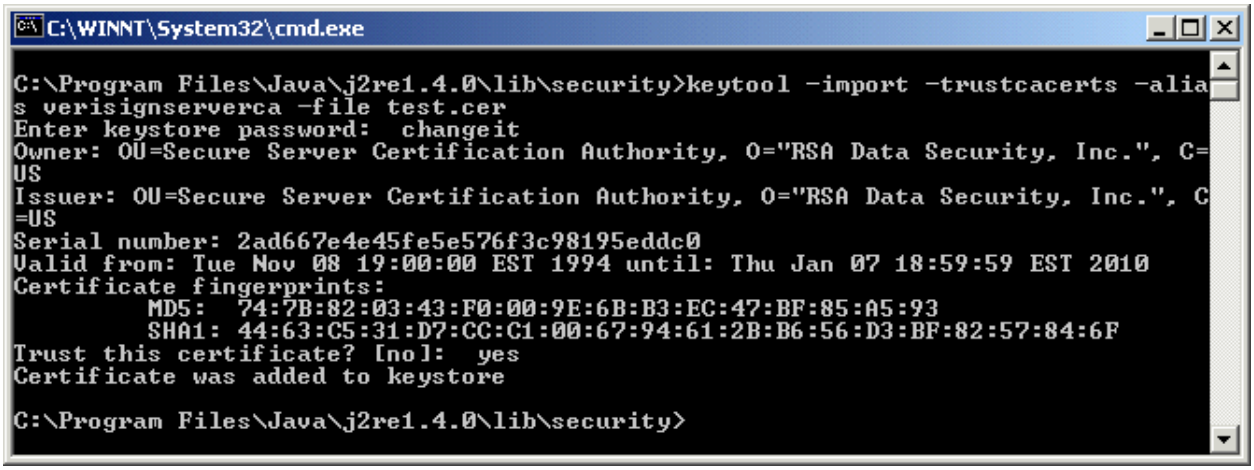

Figure 14 - Adding A Certificate

The end result of these operations is that the cacerts file will contain those certificates that match your organization's policy. This file should be distributed throughout your network and permissions should be set to prevent users from modifying this file.

Appendix B: Netscape Security References

http://channels.netscape.com/ns/browsers/default.jsp
Netscape's Browser Central – the home page for the Netscape browser.

http://wp.netscape.com/security/index.html
Netscape's Security Center – the home page for security information and updates.

http://java.sun.com/j2se/
Sun's Java 2 Standard Edition – the home page for the Java component included with Netscape.

Pistoia, Marco; Reller, Duane F., et. al., Java 2 Network Security, Prentice Hall, 1999
Explains the Java 2 security model and provides more information on Java Security.

http://www.w3.org/P3P/
Home of the Platform for Privacy Preferences (P3P) Project

http://www.c3i.osd.mil/org/cio/doc/mobile-code11-7-00.html
Policy Guidance for use of Mobile Code Technologies in Department of Defense (DoD) Information Systems

Appendix C: Sample Logon Script

The Visual Basic script associated with this document should help in setting Netscape settings throughout a network of Windows 2000 machines to match the recommendations provided here. To use this script you should do the following:

1. Thoroughly read this entire document and understand what options you would like to set in Netscape.
2. Create your script as a .vbs file by modifying this script to reflect your desired settings.
3. Test that your script works as intended in your environment.
4. Install your script so that it runs as a logon script for those users for whom you would like to enforce these settings.

```
' Netscape Reconfiguration Script Version 1.0
' This script is part of the Netscape 7.0 Configuration Guide at www.nsa.gov

' SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING,
' BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
' A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED.  IN NO EVENT SHALL THE
' CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
' EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT
' OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
' INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
' STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
' OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH
' DAMAGE.

' By removing or commenting the 2 lines below, you are signifying assent to the above
disclaimer.
MsgBox "You must first read this script's legal notice and signify assent before it
will work."
WScript.Quit(0)
' Stop removing lines here.

'Set up the Settings array to hold the Netscape preferences
Dim Settings(60,2)

' |\
' | \
' |  } START
' | /
' |/
' To customize this startup script, begin here.  The two customizations to
' this file that are recommended are:
' 1. Changing a value - change the value assigned to Settings(length,2) to
'    the setting you choose.
' 2. Not enforcing a setting - if you don't want a particular setting to
'    be set for your users, comment out all the lines of its block.

' Begin SSL Protocols

' SSL2 Cryptographic Protocol
' recommended value false
length=length+1
Settings(length,1)="security.enable_ssl2"
Settings(length,2)="false"

' SSL3 Cryptographic Protocol
' recommended value true
```

```
length=length+1
Settings(length,1)="security.enable_ssl3"
Settings(length,2)="true"

' TLS Cryptographic Protocol
' recommended value true
length=length+1
Settings(length,1)="security.enable_tls"
Settings(length,2)="true"

' End SSL Protocols

' Begin SSL2 Ciphersuites

' 128 bit RC4 - recommended true
length=length+1
Settings(length,1)="security.ssl2.rc4_128"
Settings(length,2)="true"

' 128 bit RC2 - recommended true
length=length+1
Settings(length,1)="security.ssl2.rc2_128"
Settings(length,2)="true"

' Triple DES - recommended true
length=length+1
Settings(length,1)="security.ssl2.des_ede3_192"
Settings(length,2)="true"

' DES - recommended true
length=length+1
Settings(length,1)="security.ssl2.des_64"
Settings(length,2)="true"

' 40 bit RC4 - recommended true
length=length+1
Settings(length,1)="security.ssl2.rc4_40"
Settings(length,2)="true"

' 40 bit RC2 - recommended true
length=length+1
Settings(length,1)="security.ssl2.rc2_40"
Settings(length,2)="true"

' End SSL2 Ciphersuites

' Begin SSL3/TLS Ciphersuites

' 128 bit RC4 and MD5 MAC - recommended true
length=length+1
Settings(length,1)="security.ssl3.rsa_rc4_128_md5"
Settings(length,2)="true"

' FIPS 140-1 compliant Triple DES and SHA-1 MAC - recommended true
length=length+1
Settings(length,1)="security.ssl3.rsa_fips_des_ede3_sha"
Settings(length,2)="true"

' Triple DES and SHA-1 MAC - recommended true
length=length+1
Settings(length,1)="security.ssl3.rsa_des_ede3_sha"
Settings(length,2)="true"
```

```
' FIPS 140-1 compliant DES and SHA-1 MAC - recommended false
length=length+1
Settings(length,1)="security.ssl3.rsa_fips_des_sha"
Settings(length,2)="false"

' DES and SHA-1 MAC - recommended false
length=length+1
Settings(length,1)="security.ssl3.rsa_des_sha"
Settings(length,2)="false"

' 56 bit RC4 and SHA-1 MAC - recommended false
length=length+1
Settings(length,1)="security.ssl3.rsa_1024_rc4_56_sha"
Settings(length,2)="false"

' DES in CBC Mode and SHA-1 MAC - recommended false
length=length+1
Settings(length,1)="security.ssl3.rsa_1024_des_cbc_sha"
Settings(length,2)="false"

' 40 bit RC4 and MD5 MAC - recommended false
length=length+1
Settings(length,1)="security.ssl3.rsa_rc4_40_md5"
Settings(length,2)="false"

' 40 bit RC2 and MD5 MAC - recommended false
length=length+1
Settings(length,1)="security.ssl3.rsa_rc2_40_md5"
Settings(length,2)="false"

' No encryption and MD5 MAC - recommended false
length=length+1
Settings(length,1)="security.ssl3.rsa_null_md5"
Settings(length,2)="false"

' End SSL3/TLS Ciphersuites

' Begin SSL Warnings

' warn me when loading a page that supports encryption
' recommended value false
length=length+1
Settings(length,1)="security.warn_entering_secure"
Settings(length,2)="false"

' warn me when loading a page that supports low-grade encryption
' recommended value true
length=length+1
Settings(length,1)="security.warn_entering_weak"
settings(length,2)="true"


' warn me when leaving a page that supports encryption
' recommended value true
length=length+1
Settings(length,1)="security.warn_leaving_secure"
settings(length,2)="true"

' warn me when sending form data from an unencrypted page
' to an unencrypted page
' recommended value true
length=length+1
Settings(length,1)="security.warn_submit_insecure"
```

```
settings(length,2)="true"

' warn me when viewing a page with an encrpyted/unencrypted mix
' recommended value true
length=length+1
Settings(length,1)="security.warn_viewing_mixed"
settings(length,2)="true"

'End SSL Warnings

' OCSP: use OCSP to validate only certificates that specify an OCSP service URL
length=length+1
Settings(length,1)="security.OCSP.enabled"
Settings(length,2)=1


' Begin Proxy Settings

' Proxy Autoconfig Settings
' To configure this, either uncomment the proxy autoconfig section
' and fix the url, or uncomment the no proxy use section.

'' This block can be used for a proxy autoconfig script.
'length=length+1
'Settings(length,1)="network.proxy.autoconfig_url"
'Settings(length,2)="""http://mylocalserver/proxyautoconfig.js"""
'length=length+1
'Settings(length,1)="network.proxy.type"
'Settings(length,2)=2

'' This block can be used for no proxy use.
'length=length+1
'Settings(length,1)="network.proxy.type"
'Settings(length,2)=0

' End Proxy Settings

' Use Netscape's plug-in finder service when seeking plug-ins
' recommended value - true
length=length+1
Settings(length,1)="application.use_ns_plugin_finder"
Settings(length,2)="true"

' When starting a download
' Recommended values 1 (Open a progress dialog) or 0 (Open the download manager)
length=length+1
Settings(length,1)="browser.downloadmanager.behavior"
Settings(length,2)=1

' Enable Java
' recommended value - true
length=length+1
Settings(length,1)="security.enable_java"
Settings(length,2)="true"

' Enable XSLT
' recommended value - false
length=length+1
Settings(length,1)="xslt.enabled"
Settings(length,2)="false"

' Enable Javascript for Navigator
' recommended value - true
```

```
length=length+1
Settings(length,1)="javascript.enabled"
Settings(length,2)="true"

' Begin JavaScript features

' Note that the JavaScript settings are unchecked in the GUI to disable them,
' but in the configuration file are implemented by setting a disable feature
' to true.

' Javascript: Do not allow Webpages to hide the status bar
' recommended value true
length=length+1
Settings(length,1)="dom.disable_window_open_feature.status"
Settings(length,2)="true"

' Javascript: Do not allow Webpages to change the status bar text
' recommended value true
length=length+1
Settings(length,1)="dom.disable_window_status_change"
Settings(length,2)="true"

' Javascript: Do not allow Webpages read cookies
' recommended value true
length=length+1
Settings(length,1)="dom.disable_cookie_get"
Settings(length,2)="true"

' Javascript: Do not allow Webpages to create or modify cookies
' recommended value true
length=length+1
Settings(length,1)="dom.disable_cookie_set"
Settings(length,2)="true"

' End JavaScript features

' Enable Update Notifications
' recommended value false
length=length+1
Settings(length,1)="update_notifications.enabled"
Settings(length,2)="false"

' Enable automatic software installation
' recommended value false
length=length+1
Settings(length,1)="xpinstall.enabled"
Settings(length,2)="false"

' Begin Cookie settings

' Determine cookie behavior
' Recommended value - 3, use P3P settings to determine cookie behavior
' other reasonable values:
' 1, cookies only from originating website
' 2, disable all cookies
length=length+1
Settings(length,1)="network.cookie.cookieBehavior"
Settings(length,2)=3

' Determine P3P Settings
' the following two groups correspond to the high predefined privacy level
length=length+1
Settings(length,1)="network.cookie.p3p"
```

```
Settings(length,2)="""frfradaa"""

length=length+1
Settings(length,1)="network.cookie.p3plevel"
Settings(length,2)=2

' the following two groups correspond to a custom privacy level
' length=length+1
' Settings(length,1)="network.cookie.p3p"
' Settings(length,2)="""drrrrrdr"""

' length=length+1
' Settings(length,1)="network.cookie.p3plevel"
' Settings(length,2)=3

' End Cookie settings

' Automatically save form data when completing forms
' Recommended value - false
length=length+1
Settings(length,1)="wallet.captureForms"
Settings(length,2)="false"

' Remember Passwords Using the Password Manager
' No Recommended Value, code as is will disable this feature
' length=length+1
' Settings(length,1)="signon.rememberSignons"
' Settings(length,2)="false"

' Use Encryption vs. Obscuring
' Recommended value - true
length=length+1
Settings(length,1)="wallet.crypto"
Settings(length,2)="true"

' Master Password Usage
' Recommended value - 2, ask for password every X minutes
length=length+1
Settings(length,1)="security.ask_for_password"
Settings(length,2)=2

' Master Password Timeout (in minutes)
' Recommended value - 15
length=length+1
Settings(length,1)="security.password_lifetime"
Settings(length,2)=15



'   /--\
'  /    \
'  |STOP|
'  \    /
'   \--/
'
' To customize this startup script for use with the Netscape 7.0
' configuration guide, you should not need to modify anything after
' this point.

Set WshShell=WScript.CreateObject("WScript.Shell")
Set WshFSO=WScript.CreateObject("Scripting.FileSystemObject")

Sub MyAppendPrefs(MyFileLoc)
```

```
          If WshFSO.FileExists(MyFileLoc&"\Prefs.js") Then
             Set MyPrefsFile=WshFSO.OpenTextFile(MyFileLoc&"\Prefs.js", 8)
             For i=1 to length
                   MyPrefsFile.WriteLine "user_pref(" & Chr(34) & Settings(i,1) &
Chr(34) & ", " & Settings(i,2) & ");"
             Next
          End If
End Sub

'Find the Application Data folder, in Win2K found at a location like c:\documents and
settings\username\Application Data
MyAppData=WshShell.RegRead("HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersio
n\Explorer\Shell Folders\AppData")

'Find the subfolder of Application Data where Netscape 7 keeps its profiles
Set MyProfile=WshFSO.GetFolder(MyAppData & "\Mozilla\Profiles")

'Find any directory two directories down from there.
'The first directory is the profile name, the second is a hard to guess name.

For Each MyProfileName in MyProfile.SubFolders
          For Each PrefsDirectory in MyProfileName.SubFolders
'With each such directory, append the administrative preferences to this file.
             Call MyAppendPrefs(PrefsDirectory)
          Next
Next
```