

Loading Certificates on Protected Web Sites

Developed by WebWorks

July 7, 2009

Table of Contents

<i>Loading Certificates on Protected Web Sites</i> _____	1
Introduction _____	1
Site Security Certificate Not in Browser _____	1
Add an Exception (Mozilla Firefox only) _____	1
Create a Trusted Site (IE only) _____	3
<i>Loading the Site Certificate into Internet Explorer</i> _____	7
<i>Loading the Site Certificate into Mozilla Firefox</i> _____	14
<i>Other Common Error Messages</i> _____	19
Switching from HTTP to HTTPS Pages with IE _____	19
Accessing a Protected Site with IE _____	19
<i>APPENDIX A: Loading Certificates on Protected Web Sites (condensed)</i> _____	A-1
Site Security Certificate Not in Browser _____	A-1
Add an Exception (Mozilla Firefox only) _____	A-1
Create a Trusted Site (IE only) _____	A-1
Loading the Site Certificate into Internet Explorer _____	A-1
Loading the Site Certificate into Mozilla Firefox _____	A-2
Other Common Error Messages _____	A-2
Switching from HTTP to HTTPS Pages with IE _____	A-2
Accessing a Protected Site with IE _____	A-2

Table of Figures

Figure 1. Secure Connection Failed Notice	2
Figure 2. Secure Connection Failed Notice (reloaded)	2
Figure 3. Add Security Exception Window	2
Figure 4. Add Security Exception Window (reloaded)	3
Figure 5. Internet Options Window	3
Figure 6. Internet Options Window Security Tab	4
Figure 7. Internet Options Window (Trusted sites)	4
Figure 8. Trusted sites Window	5
Figure 9. Trusted sites Window (URL entered)	5
Figure 10. Trusted sites Window (URL added as Trusted site)	6
Figure 11. Trusted sites Window (deletion selected)	6
Figure 12. CA Certificate Download Page	7
Figure 13. Download Certificate Window	7
Figure 14. File Download Window	8
Figure 15. Save As Window	8
Figure 16. Download Complete Window	8
Figure 17. Internet Options Window	9
Figure 18. Internet Options Window Content Tab	9
Figure 19. Certificates Window	10
Figure 20. Certificate Import Wizard	10
Figure 21. Certificate Import Wizard (reloaded)	10
Figure 22. Open Window	11
Figure 23. Certificate Import Wizard (reloaded)	11
Figure 24. Certificate Import Wizard (reloaded)	12
Figure 25. Certificate Import Wizard (reloaded)	12
Figure 26. Success Window	12
Figure 27. Security Alert Window	13
Figure 28. Security Warning Window	13
Figure 29. DoD Certificate Download Page	14
Figure 30. File Download Window	14
Figure 31. Downloading Certificate Window	14
Figure 32. Save As Window	15
Figure 33. Download Complete Window	15

<i>Figure 34. Options Window</i>	15
<i>Figure 35. Options Window Advanced Screen</i>	16
<i>Figure 36. Options Window Encryption Tab</i>	16
<i>Figure 37. Certificate Manager Window</i>	17
<i>Figure 38. Select File Window</i>	17
<i>Figure 39. Select File Window (reloaded)</i>	17
<i>Figure 40. Downloading Certificate Window</i>	18
<i>Figure 41. Certificate Viewer Window</i>	18
<i>Figure 42. Security Alert Window</i>	18
<i>Figure 43. Security Warning Window</i>	19
<i>Figure 44. Security Warning</i>	19
<i>Figure 45. Security Alert</i>	19
<i>Figure 46. Choose a Digital Certificate Window</i>	20
<i>Figure 47. Security Certificate Problem Notice</i>	20
<i>Figure 48. Security Warning Window</i>	21
<i>Figure 49. Security Alert Window</i>	21
<i>Figure 50. Choose a Digital Certificate Window</i>	21

Loading Certificates on Protected Web Sites

Introduction

Some users will see unexpected messages when attempting to view a protected web site, particularly if this is their first attempt to access a protected site. These messages typically occur because some step in the certificate installation process or accompanying browser configuration setup has been omitted. This document covers some of the most common problems encountered when using Internet Explorer (version 6.0 and 7.0) and Mozilla Firefox (Version 3.0). Other browsers may have similar problems.

There are two main steps that must be completed before you can access a protected web site.

1. Install the site security certificate in the browser.
2. Install your personal PKI certificate in the browser.

Please contact your local IT Support office for any assistance you may need with these procedures.

This document assumes that you have already correctly loaded your personal PKI certificate into the browser and are still having receiving error messages.



Note that if you are experienced with this type of web activity, there is a one-page quick reference at the end of this document.

Site Security Certificate Not in Browser

The following are the messages commonly seen when the protected web site's security certificate is not correctly installed in a browser. In Internet Explorer (Version 6.0), this will likely to be a *Choose a digital certificate* window. In Mozilla Firefox (Version 3.0), you might receive a *Secure Connection Failed* message. You can test whether this applies to you by visiting this page: <https://www.iad.gov/events/conferences/register/LoginType.cfm>.

If you *do not* receive a message, no action is necessary.

The messages are meant to inform you that the protected web site's security certificate was not included by default in your browser. There are two easy ways to avoid these messages:

1. Add an exception for the web site (Mozilla Firefox only) or create a Trusted Site (IE only).
2. Import a DoD Root CA 2 Certificate (preferred).

While adding an exception is the faster, easier process, you might have to repeat the process for multiple protected DoD web sites. Importing the DoD Root CA 2 Certificate will take about 2 minutes, but it is the more thorough solution. You should only have to import it once per browser. The DoD Root CA 2 Certificate will let your browser recognize many protected DoD web sites and prevent unwanted messages.

Guidelines are given for all the above procedures in both Firefox and IE. Other browsers should have similar procedures. Again, contact your local IT Support office for any assistance you may need.

Add an Exception (Mozilla Firefox only)

If you receive a *Secure Connection Failed* (Figure 1) message in Mozilla Firefox, you have the option of simply adding an *Exception*, thereby making it a *Trusted Site*. To do so, complete the following steps:



Figure 1. Secure Connection Failed Notice

1. Click *Or you can add an exception.* The page reloads (Figure 2).



Figure 2. Secure Connection Failed Notice (reloaded)

2. Click *Add Exception.* The *Add Security Exception* window opens (Figure 3).

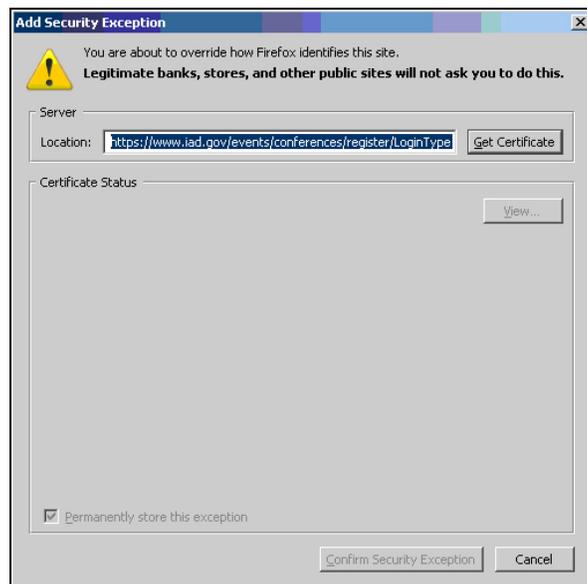


Figure 3. Add Security Exception Window

3. Click *Get Certificate*. The window reloads (Figure 4).

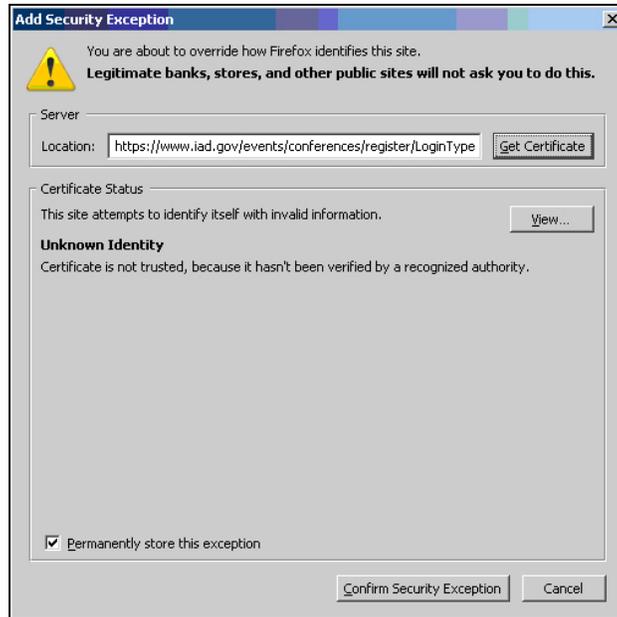


Figure 4. Add Security Exception Window (reloaded)

4. Ensure that the *Permanently store this exception* box is checked and then click *Confirm Security Exception*.

Create a Trusted Site (IE only)

1. Go to *Tools > Internet Options* (Figure 5).



Figure 5. Internet Options Window

2. Select the *Security* tab (Figure 6).

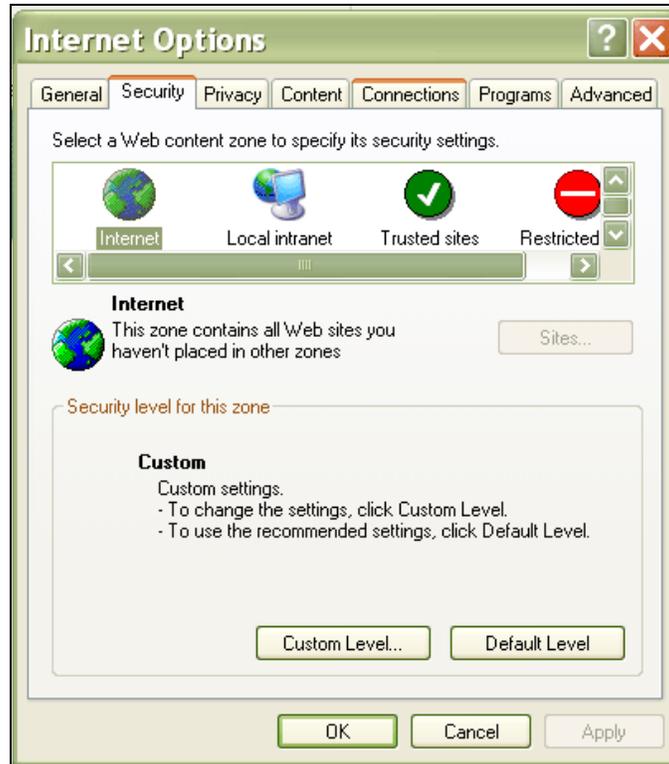


Figure 6. Internet Options Window Security Tab

3. Click *Trusted Sites* (Figure 7).

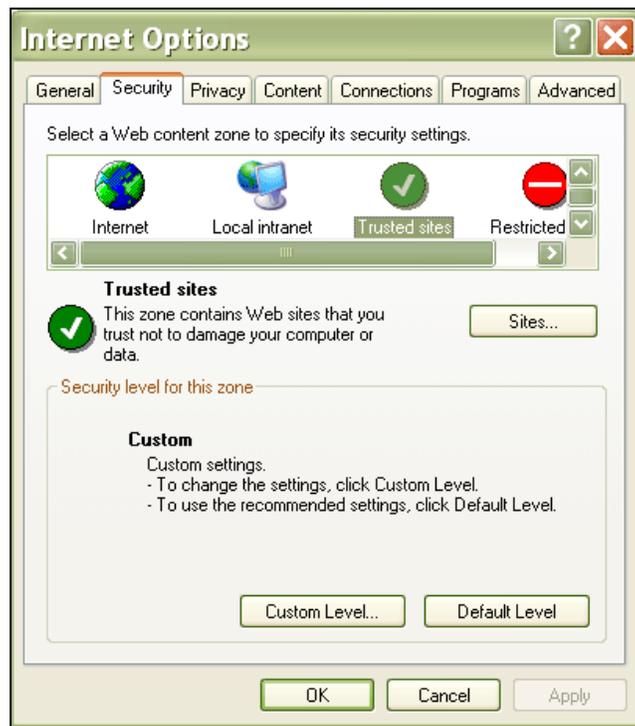


Figure 7. Internet Options Window (Trusted sites)

- To create a *Trusted Site*, click *Sites*. The *Trusted Sites* window opens (Figure 8).

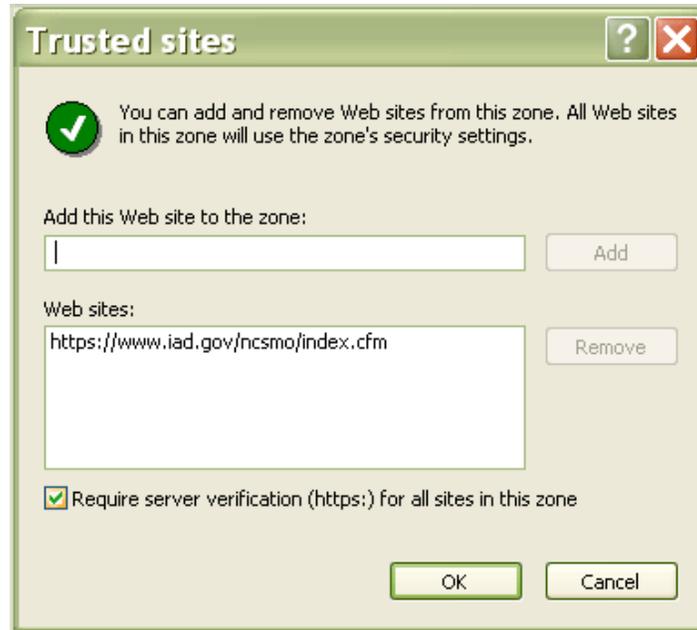


Figure 8. Trusted sites Window

- Enter the *URL* of the desired site (Figure 9).

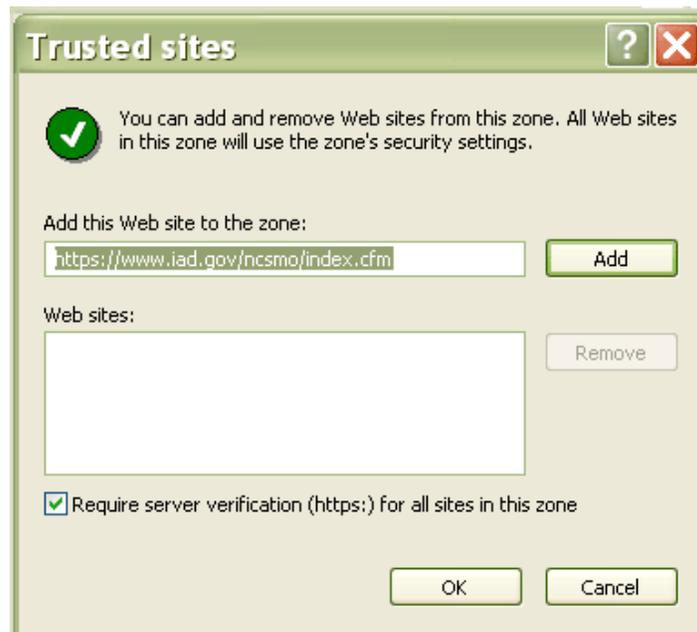


Figure 9. Trusted sites Window (URL entered)

- Click *Add*. The site is listed in the *Trusted sites* text box (Figure 10).

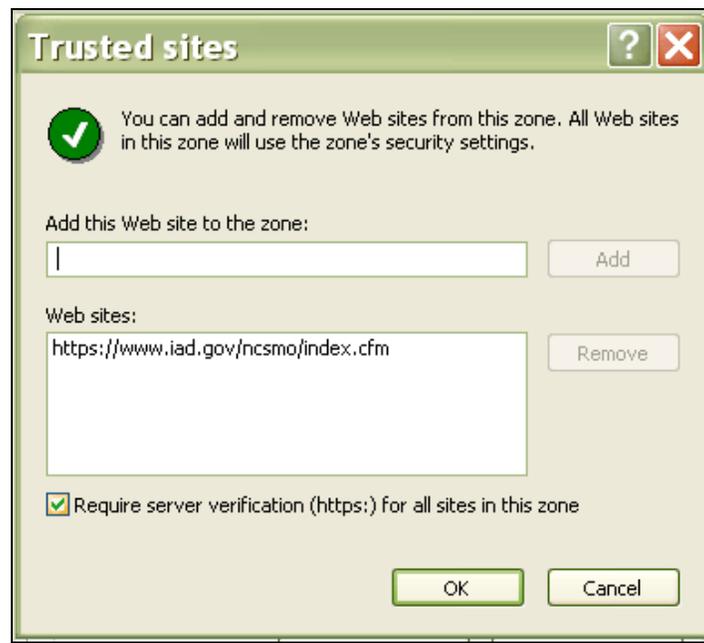


Figure 10. Trusted sites Window (URL added as Trusted site)

7. You can also remove *Trusted sites* by highlighting a URL in the *Web sites* text box and clicking *Remove* (Figure 11).

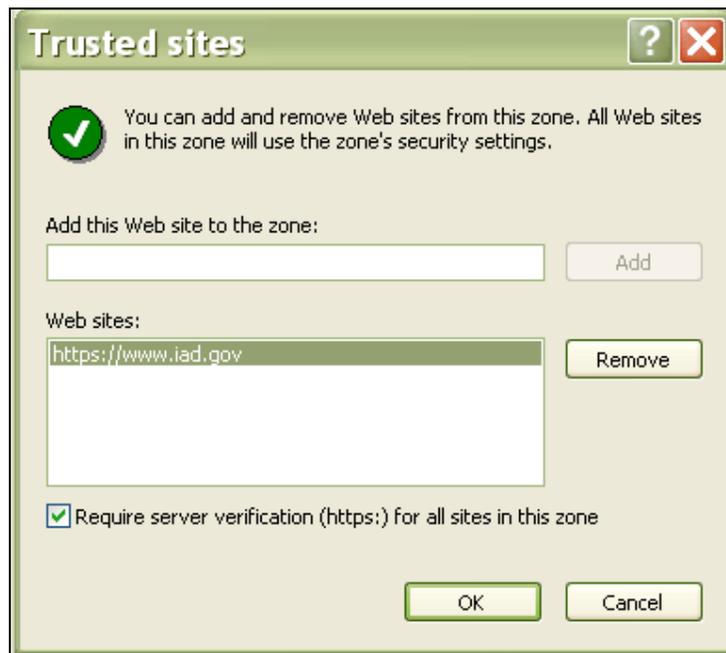


Figure 11. Trusted sites Window (deletion selected)

8. Check *Require server verification (https:) for all sites in this zone*.

Loading the Site Certificate into Internet Explorer

1. Open Internet Explorer.
2. Navigate to the following URL: <http://dodpki.c3pki.chamb.disa.mil/rootca.html> (Figure 12).



Figure 12. CA Certificate Download Page

3. Select **Download Root CA 2 Certificate**. The **Downloading Certificate** window appears. If instead a **File Download** window appears, skip to Step 6.
4. Select all three check boxes and click **OK** (Figure 13).

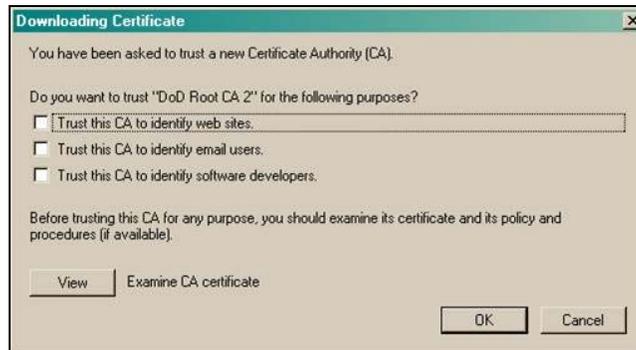


Figure 13. Download Certificate Window

5. Close and re-open your browser. Test that the import was successful by navigating to <https://www.iad.gov/events/conferences/register/LoginType.cfm>. If successful, you will not receive a pop-up window.
6. If a **File Download** window appears (Figure 14), click **Save**. Select a download location (Figure 15). Keep the default name, which at the time of this writing is **rel3_dodroot_2048.p7b**. Click **Save**. When the file is saved (Figure 15), click **Close** (Figure 16). (Window may close automatically.)



Figure 14. File Download Window

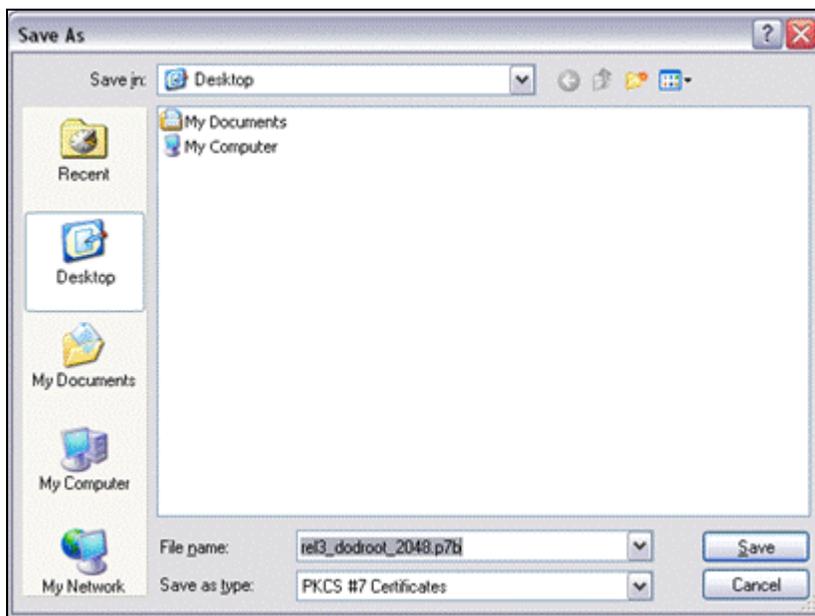


Figure 15. Save As Window

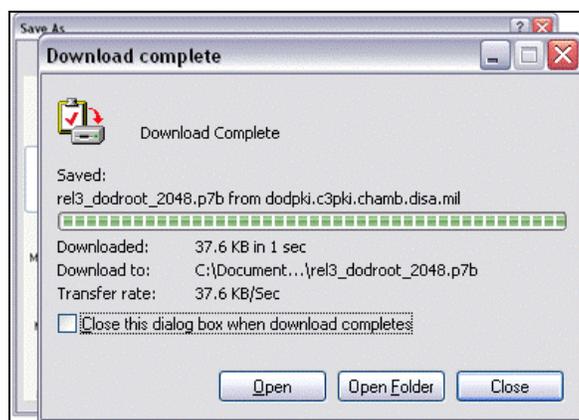


Figure 16. Download Complete Window

7. Select **Tools > Internet Options**. The **Internet Options** window opens (Figure 17).



Figure 17. Internet Options Window

8. Click the **Content** tab, and then the **Certificates** button (Figure 18). The **Certificates** window opens (Figure 19).



Figure 18. Internet Options Window Content Tab

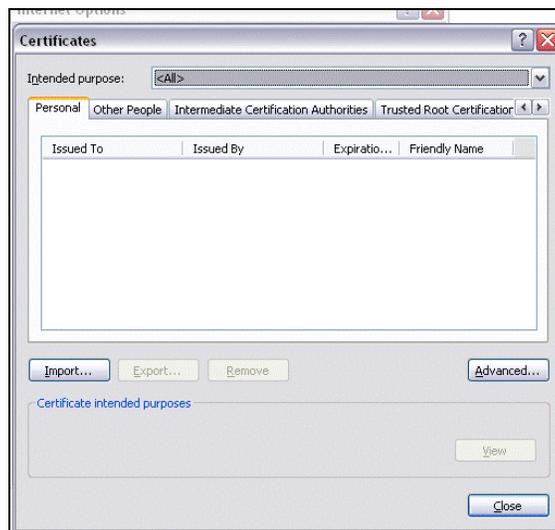


Figure 19. Certificates Window

9. Click the **Import** button. The **Certificate Import Wizard** window opens (Figure 20).



Figure 20. Certificate Import Wizard

10. Click **Next**. The page reloads (Figure 21).



Figure 21. Certificate Import Wizard (reloaded)

11. Click **Browse**. The **Open** window displays (Figure 22).

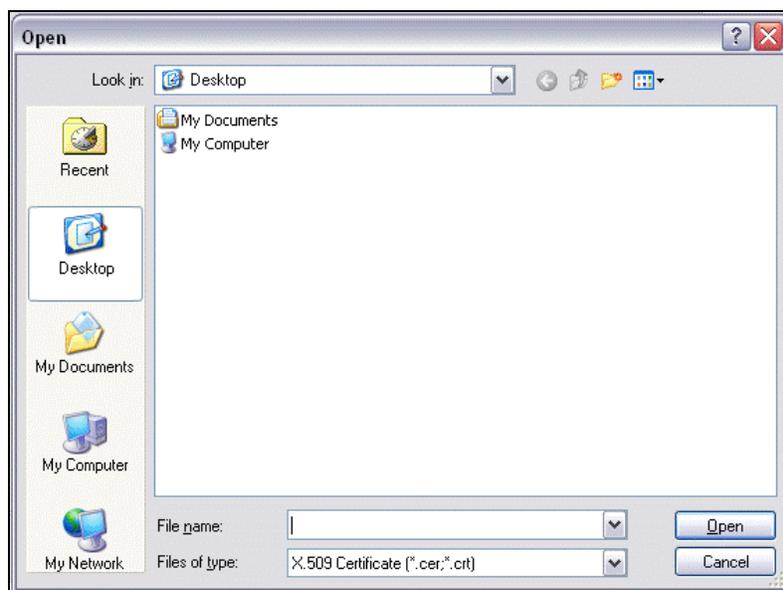


Figure 22. Open Window

12. Navigate to the directory where you saved the Root CA 2 Certificate.
13. Change the *Files of Type* option to *All Files (*.*)*.
14. Select the certificate file (e.g., *rel3_dodroot_2048.p7b*) and click *Open*. The page reloads and shows the file as selected (Figure 23).

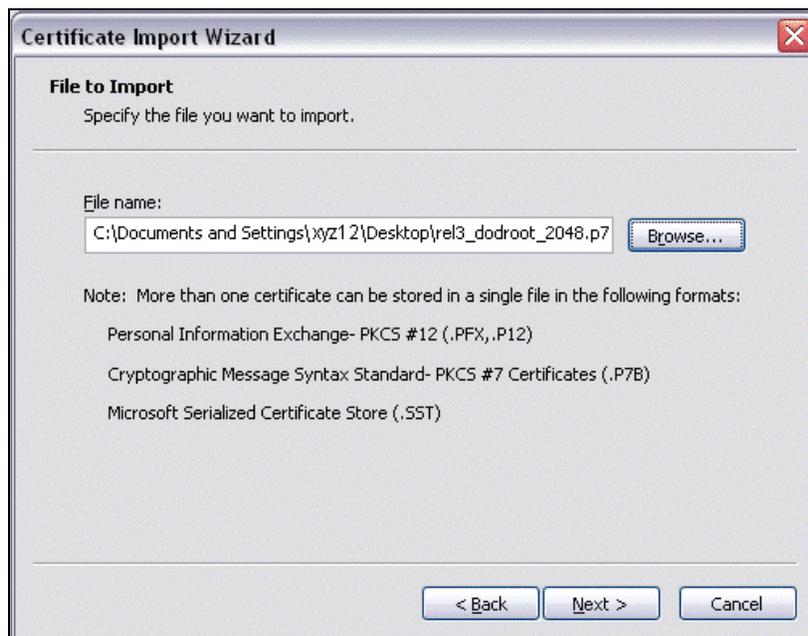


Figure 23. Certificate Import Wizard (reloaded)

15. Click *Next*. The page reloads (Figure 24).

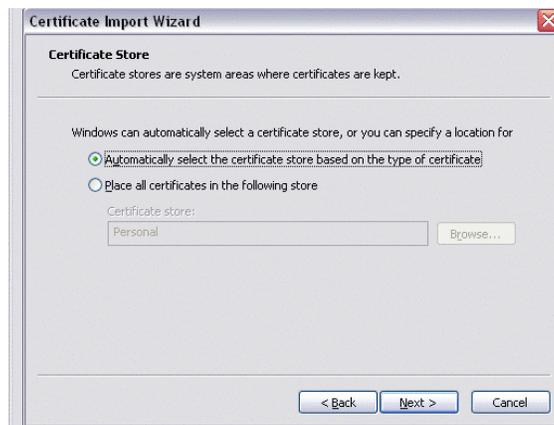


Figure 24. Certificate Import Wizard (reloaded)

16. Select *Automatically select the certificate store based on the type of certificate* and then click *Next*. The page reloads (Figure 25).



Figure 25. Certificate Import Wizard (reloaded)

17. Figure 26). Click *OK*. You may close any of the remaining option windows.



Figure 26. Success Window

18. Close and re-open your browser. Test that the import was successful by navigating to <https://www.iad.gov/events/conferences/register/LoginType.cfm>. If successful, you will not receive a pop-up window, although you may see a *Security Alert* like those below. Click *OK* or *Yes*.



Figure 27. Security Alert Window



Figure 28. Security Warning Window

Loading the Site Certificate into Mozilla Firefox

1. Open Mozilla Firefox.
2. Navigate to the following URL: <http://dodpki.c3pki.chamb.disa.mil/rootca.html> (Figure 29).



Figure 29. DoD Certificate Download Page

3. Select *Download Root CA 2 Certificate*. A "File Download" window appears (Figure 30). Click *Open*.



Figure 30. File Download Window

4. If, instead, a *Downloading Certificate* window opens (Figure 31) that shows three checkboxes, as it did in IE, select all three boxes and click *OK*.

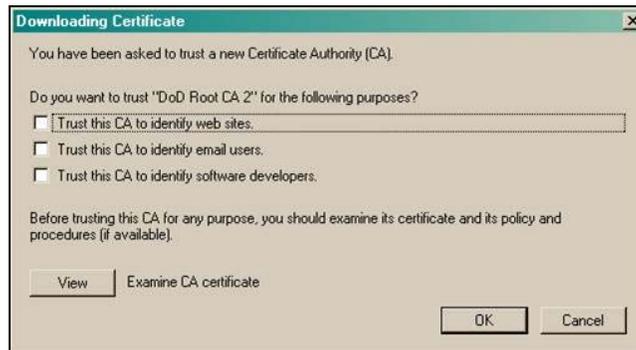


Figure 31. Downloading Certificate Window

5. When the *Save As* window opens (Figure 32), select a download location and click *Save* again. Keep the default name, which at the time of this writing is *rel3_dodroot_2048.p7b*.

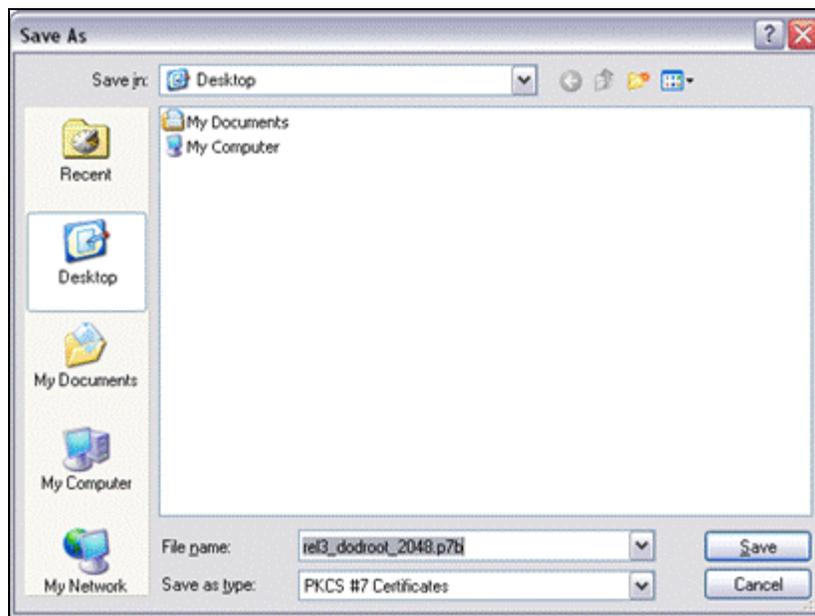


Figure 32. Save As Window

5. When the file is saved, click *Close* (Figure 33). (Window may close automatically.)



Figure 33. Download Complete Window

6. Select *Tools > Options*. The *Options* window opens (Figure 34).



Figure 34. Options Window

7. Click the *Advanced* icon. The window reloads (Figure 35).

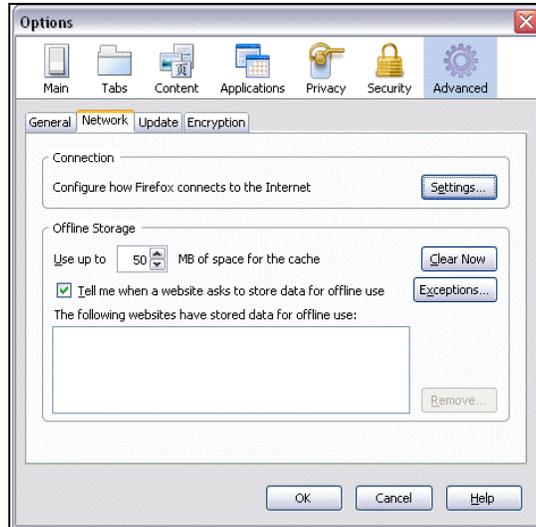


Figure 35. Options Window Advanced Screen

8. Click the *Encryption* tab. The window reloads (Figure 36).

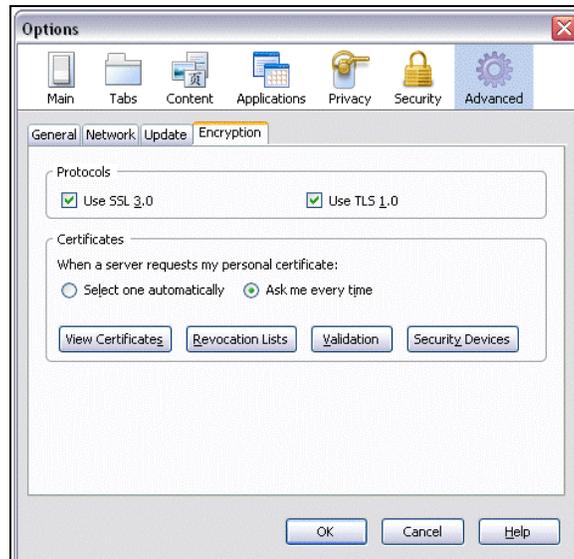


Figure 36. Options Window Encryption Tab

9. Click *View Certificates*. The *Certificate Manager* window opens (Figure 37).

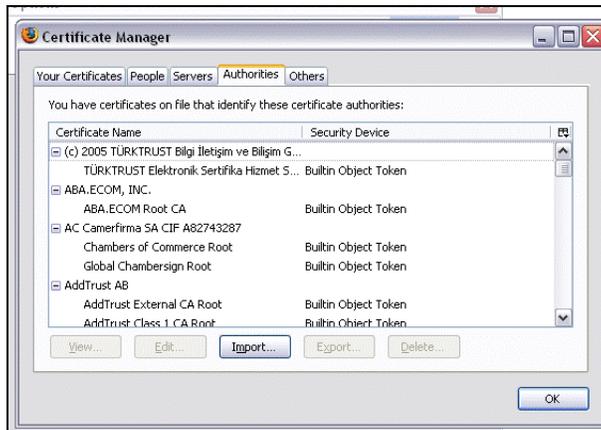


Figure 37. Certificate Manager Window

10. Click *Import*. The *Select File containing CA certificate(s) to import* window opens (Figure 38).

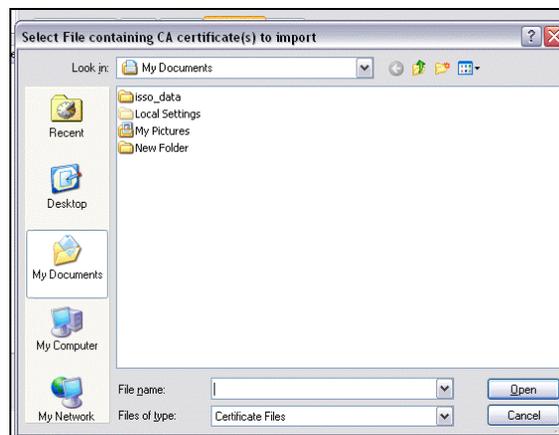


Figure 38. Select File Window

11. Navigate to the directory where you saved the *Root CA 2 Certificate*.

12. Change the *Files of type* option to *All Files*.

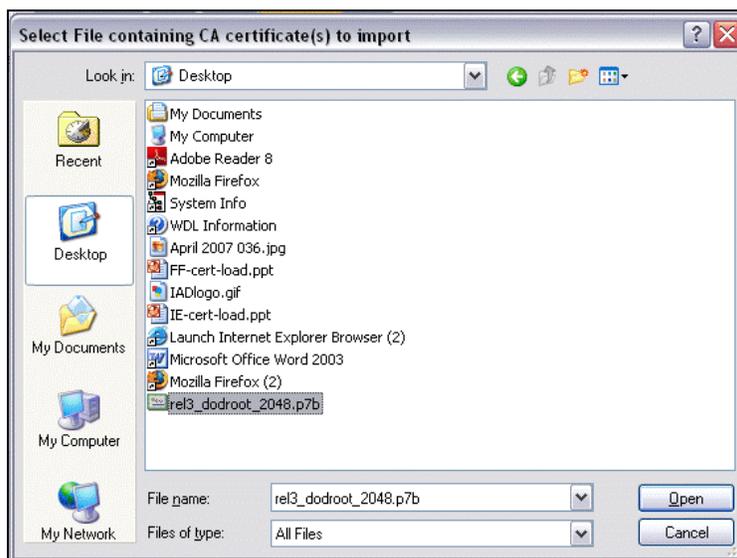


Figure 39. Select File Window (reloaded)

13. Select the certificate file (e.g., *rel3_dodroot_2048.p7b*) and click *Open*. The certificate is downloaded (Figure 40). Click *View*. The page reloads and shows the file as selected (Figure 41).



Figure 40. Downloading Certificate Window

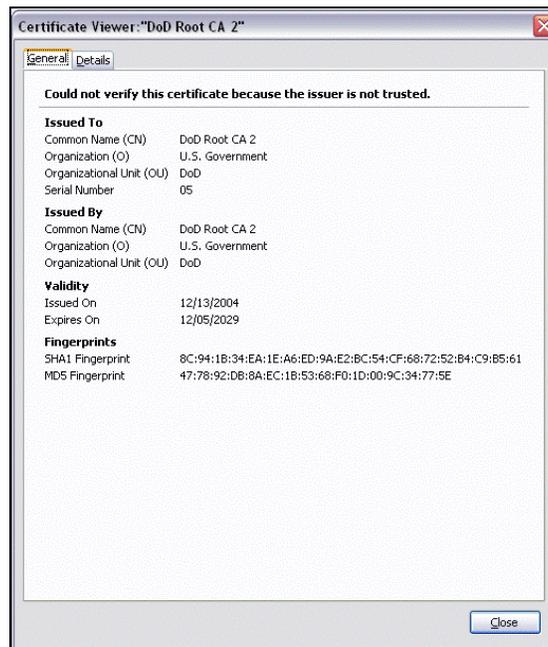


Figure 41. Certificate Viewer Window

14. If prompted, enter the password you used for your individual DoD PKI certificate.
15. When finished, close and re-open your browser.
16. Test that the import was successful by navigating to <https://www.iad.gov/events/conferences/register/LoginType.cfm>. If successful, you will not receive a pop-up window, although you may see a *Security Alert* like those below (Figure 42, Figure 43). Click *OK* or *Yes*.



Figure 42. Security Alert Window



Figure 43. Security Warning Window

Other Common Error Messages

The following are messages that may be received even when everything is installed correctly and are usually alerts rather than error messages.

Switching from HTTP to HTTPS Pages with IE

If you enter the site URL starting with `http` instead of `https`, or if the page you're coming from had a URL starting with `http`, and the link to the secure site was coded with a relative link (like *IAD.gov* to the *NCSMO* site), you may see the following prompt. Select *Yes* to proceed.



Figure 44. Security Warning

Accessing a Protected Site with IE

When opening the site in IE (for a given session) you may be prompted to confirm that it's OK to go to a secure site.



Figure 45. Security Alert

You may then have to identify your certificate.

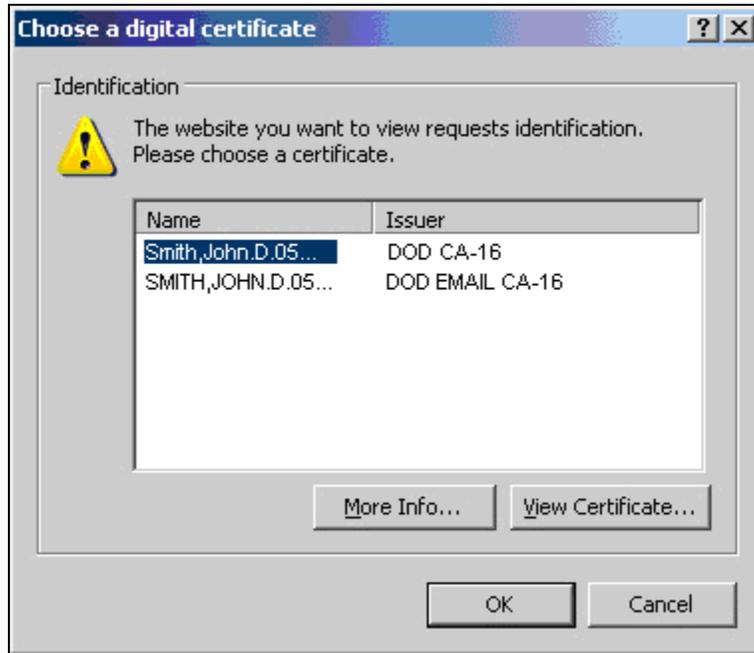


Figure 46. Choose a Digital Certificate Window

In place of the two screens above, you may also encounter the following series of prompts. On the first screen, select *Continue to this website*.



Figure 47. Security Certificate Problem Notice

Select *Yes* and then *OK* on the following screens.



Figure 48. Security Warning Window



Figure 49. Security Alert Window

Identify your personal PKI certificate when prompted.

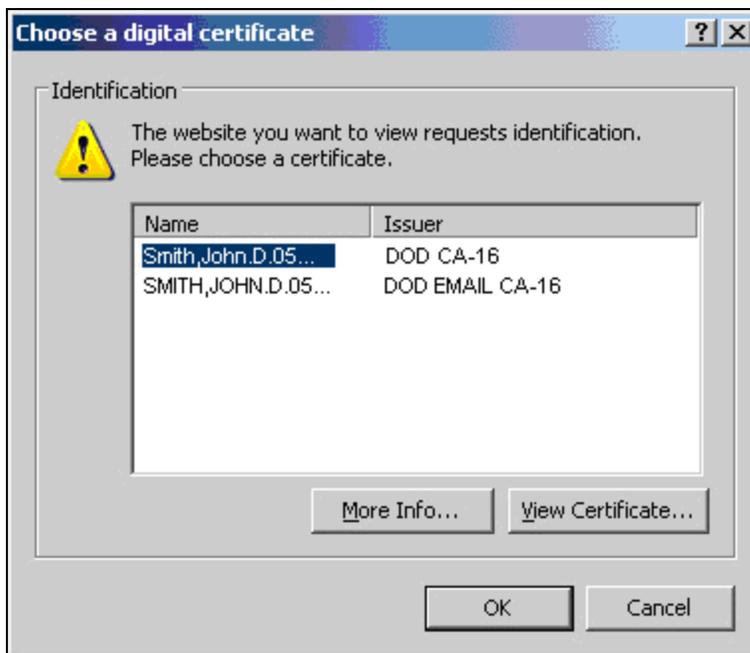


Figure 50. Choose a Digital Certificate Window

APPENDIX A: Loading Certificates on Protected Web Sites (condensed)

Site Security Certificate Not in Browser

If you get error messages it may mean that the site security certificate has not been loaded into your browser. You can check this by visiting this page: <https://www.iad.gov/events/conferences/register/LoginType.cfm>. If you *do not* receive a message, no action is necessary. There are two easy ways to avoid these messages:

1. Add an exception for the web site (Mozilla Firefox only) or create a Trusted Site (IE only).
2. Import a DoD Root CA 2 Certificate (preferred).

While adding an exception is the faster, easier process, you might have to repeat the process for multiple protected DoD web sites. Importing the DoD Root CA 2 Certificate will take about 2 minutes, but it is the more thorough solution. You should only have to import it once per browser.

Add an Exception (Mozilla Firefox only)

1. On the error window, click *Or you can add an exception*; the page reloads.
2. Click *Add Exception*; the *Add Security Exception* window opens.
3. Click *Get Certificate* the window reloads.
4. Check the *Permanently store this exception* box; click *Confirm Security Exception*.

Create a Trusted Site (IE only)

1. Go to *Tools > Internet Options*.
2. Select the *Security* tab.
3. Click *Trusted Sites*.
4. To create a *Trusted Site*, click *Sites* the *Trusted Sites* window opens.
5. Enter the *URL* of the desired site.
6. Click *Add*. The site is listed in the *Trusted sites* text box. (You can remove *Trusted sites* by highlighting a URL in the *Web sites* text box and clicking *Remove*.)
7. Check *Require server verification (https:)* for all sites in this zone.

Loading the Site Certificate into Internet Explorer

1. Open Internet Explorer.
2. Navigate to: <http://dodpki.c3pki.chamb.disa.mil/rootca.html>.
3. Select *Download Root CA 2 Certificate*; the *Downloading Certificate* window appears. If, however, a *File Download* window appears, skip to Step 6.
4. Select all three check boxes and click *OK*.
5. Close and re-open your browser.
6. Test that the import by navigating to <https://www.iad.gov/events/conferences/register/LoginType.cfm>. If successful, you will not see a pop-up window.
7. If a *File Download* window appears, click *Save*. Select a download location. Keep the default name. Click *Save*. When the file is saved, click *Close*. (Window may close automatically.)
8. Select *Tools > Internet Options*.
9. Click the *Content* tab, and then the *Certificates* button; the *Certificates* window opens.
10. Click the *Import* button; the *Certificate Import Wizard* opens.
11. Click *Next*; the page reloads.
12. Click *Browse*.
13. Navigate to the directory where you saved the Root CA 2 Certificate.
14. Change the *Files of Type* option to *All Files (*.*)*.
15. Select the certificate file and click *Open*; the page reloads and shows the file as selected.
16. Click *Next*; the page reloads.
17. Select *Automatically select the certificate store based on the type of certificate* and click *Next*; the page reloads.
18. Click *Finish*. You should see a pop-up success message. Click *OK*. Close any of the remaining option windows.
19. Close and re-open your browser.
20. Test that the import was successful by navigating to <https://www.iad.gov/events/conferences/register/LoginType.cfm>. If successful, you will not receive a pop-

up window, although you may see a *Security Alert*. Click *OK* or *Yes*.

Loading the Site Certificate into Mozilla Firefox

1. Open Mozilla Firefox.
2. Navigate to: <http://dodpki.c3pki.chamb.disa.mil/rootca.html>.
3. Select *Download Root CA 2 Certificate*. A “*File Download*” window appears.
4. Click *Save*. Select a download location and click *Save*. Keep the default name. When the file is saved, click *Close*. (Window may close automatically.)
5. Select *Tools > Options*; the *Options* window opens.
6. Click the *Advanced* icon; the window reloads.
7. Click the *Encryption* tab; the window reloads.
8. Click *View Certificates*; the *Certificate Manager* window opens.
9. Click *Import*; the *Select File containing CA certificate(s) to import* window opens.
10. Navigate to the directory where you saved the *Root CA 2 Certificate*.
11. Change the *Files of type* option to *All Files (*.*)*.
12. Select the certificate file and click *Open*. The certificate is downloaded. Click *View*; the page reloads and shows the file as selected.
13. If prompted, enter the password you used for your individual DOD PKI certificate.
14. When finished, close and re-open your browser.
15. Test that the import was successful by navigating to <https://www.iad.gov/events/conferences/register/LoginType.cfm>. If successful, you will not receive a pop-up window, although you may see a *Security Alert*. Click *OK* or *Yes*.

Other Common Error Messages

You may see some messages, usually alerts, rather than error messages, even when everything is installed correctly, for example:

Switching from HTTP to HTTPS Pages with IE

If you enter the site URL starting with [http](http://), instead of [https](https://), or if the page you’re coming from had a URL starting with [http](http://) and the link to the secure site was coded with a relative link, you may see a security warning. Select *Yes* to proceed.

Accessing a Protected Site with IE

When opening the site in IE, you may be asked to confirm that it’s OK to go to a secure site. You may then have to identify your certificate. You may also encounter a series of prompts. On the first screen, select *Continue to this website*. On the following screens, select *Yes* and then *OK*.