



General Branding And Logo Usage Guidelines

Last Updated: November 1999

Introduction

This document is intended to serve as a guide for ValiCert partners who are integrating validation capability using either the ValiCert Validator Toolkit or some ValiCert Validator Suite component(s). The requisite ValiCert Partner and 'ValiCert-Ready' logo files referenced in this document are available in gif, bmp, ai, and eps formats in a separate directory within this package. Please use these files as delineated below.

ValiCert Logo Usage

ValiCert Partner Logo

- This logo is appropriate for use by all ValiCert product and corporate partners
- Should be viewable in at least the size shown below (108 x 73 pixels)
- Should be included on ValiCert partners' corporate web pages and collateral (where applicable)
- Should be linked to <http://www.valicert.com> (when it appears on corporate web pages)



'ValiCert-Ready' Logo

- This logo should be posted in all appropriate locations within the application itself, including the following:
 - Installation splash screen (where applicable); minimum 72 x 42 pixels, as illustrated below
 - Start splash screen (where applicable); minimum 72 x 42 pixels
 - Validation configuration page (where applicable); minimum 72 x 42 pixels
 - "Help About," "About Plug-Ins," or equivalent attribution page (minimum 72 x 42 pixels)
- Should be linked to <http://www.valicert.com>
- The listed url should be <http://www.valicert.net/trendmicro>



Sample Attribution



← <http://www.valicert.com>

trademarks of ValiCert, Inc. registered in the US and other countries. Find out more about certificate validation at <http://www.valicert.net>

Sample Dialogue Boxes

Certificate Validation Configuration: Server-Based Applications

The screenshot shows the FrontPage Editor interface with a new page titled "FrontPage Editor - [New Page]". The menu bar includes File, Edit, View, Go, Insert, Format, Tools, Table, Frame, Window, and Help. A status bar at the top indicates "This page contains elements that may need to be saved or published to preview correctly." The main content area displays the "Certificate Validation Configuration" dialog box. The dialog has a title bar and a main area with the following text: "Certificate validation allows you to verify that the web servers your users attempt to access are signed with valid digital certificates. This ensures that your clients can trust the secure web servers to which they are connecting. If a client accesses a web server which has been signed with a revoked SSL certificate, InterScan WebManager will automatically terminate the connection. To get certificate validation reports and information, link to ValiCert, Inc.'s website at <http://www.valicert.net/TrendMicro>". Below this text is a section titled "Certificate Validation Setup" with a checkbox "Enable certificate validation for SSL connections:". Under this checkbox are two radio button options: "Use ValiCert Global VA ServiceSM" (which is selected) and "Use a ValiCert Enterprise VATM server on your local network:". The second option has two input fields: "IP address of local Enterprise VA server:" and "Port:" (with "80" entered). Below these is a text field for "Location of self-signed certificate for local Enterprise VA server:" with the placeholder text "[should point to file]". At the bottom of the dialog are "Save" and "Restore" buttons. The FrontPage Editor's status bar shows "Normal", "HTML", and "Preview" tabs. The Windows taskbar at the bottom shows the Start button, MaxTime, Microsoft, New P..., Inbox..., FrontPa..., Front..., and untitled... icons, along with the system clock showing 7:47 PM.

FrontPage Editor - [New Page]

File Edit View Go Insert Format Tools Table Frame Window Help

This page contains elements that may need to be saved or published to preview correctly.

Certificate Validation Configuration

Certificate validation allows you to verify that the web servers your users attempt to access are signed with valid digital certificates. This ensures that your clients can trust the secure web servers to which they are connecting. If a client accesses a web server which has been signed with a revoked SSL certificate, InterScan WebManager will automatically terminate the connection. To get certificate validation reports and information, link to ValiCert, Inc.'s website at <http://www.valicert.net/TrendMicro>

Certificate Validation Setup

☐ Enable certificate validation for SSL connections:

- ☒ Use ValiCert Global VA ServiceSM
- ☐ Use a ValiCert Enterprise VATM server on your local network:
 - IP address of local Enterprise VA server: Port:
 - Location of self-signed certificate for local Enterprise VA server:

Save Restore

Normal HTML Preview

Start MaxTime Microsoft New P... Inbox... FrontPa... Front... untitled... 7:47 PM

Certificate Validation Configuration: Client-Based Applications

ValiCert E-Mail Validator : Certificate Validation Options [X]

Validate Certificate using:

☐ ValiCert Global VA Service

☐ ValiCert VA

Port:

☐ Local Data Store

OK

Cancel

Validation Protocol & Certificate Stores:

☐ CRT

☐ OCSP

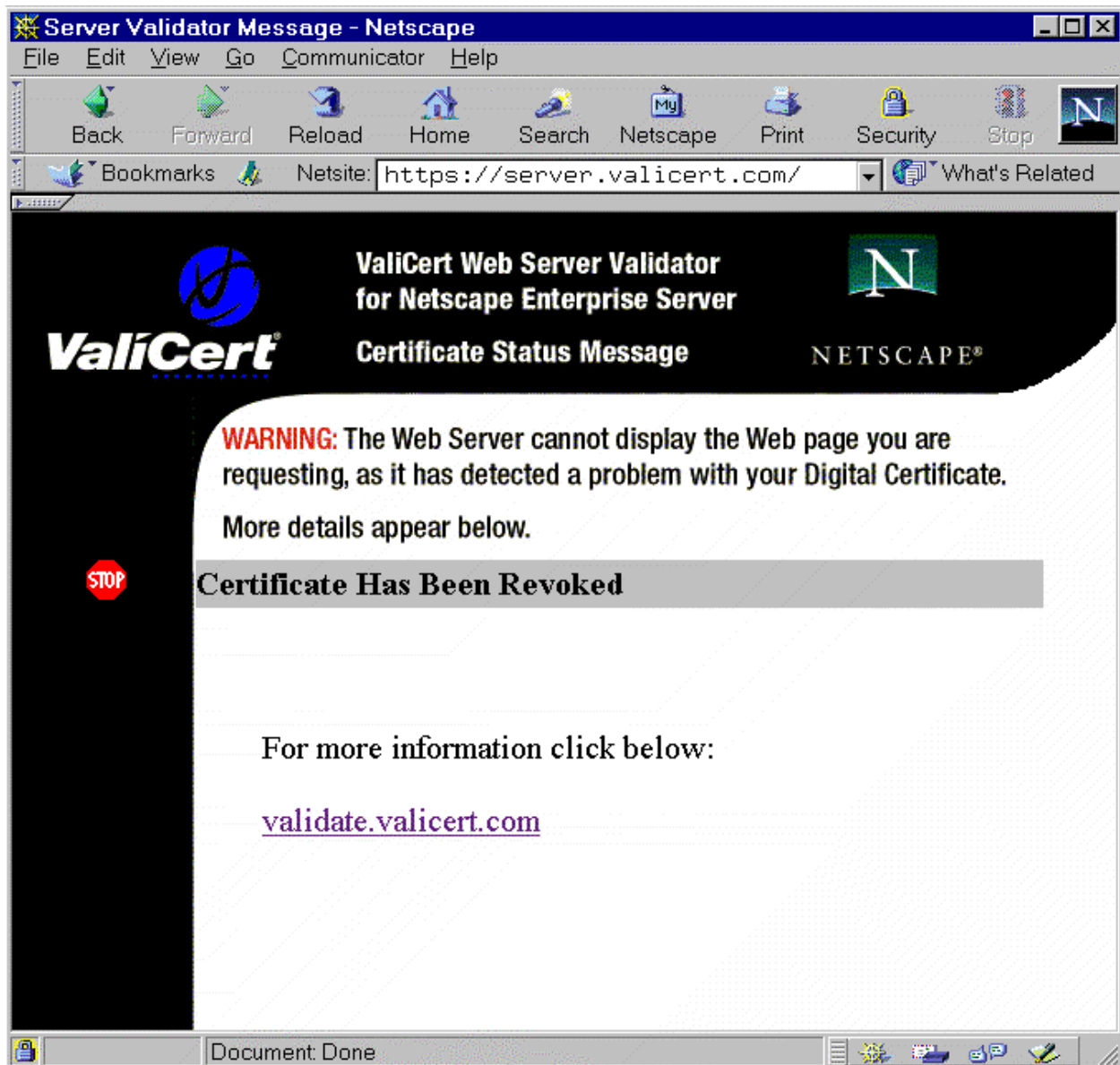
☐ CRL

ValiCert Freshness Proof Stamp

☐ Add Freshness Proof Stamp to Outgoing Messages

☐ Trust Freshness Proof Stamp of Incoming Messages

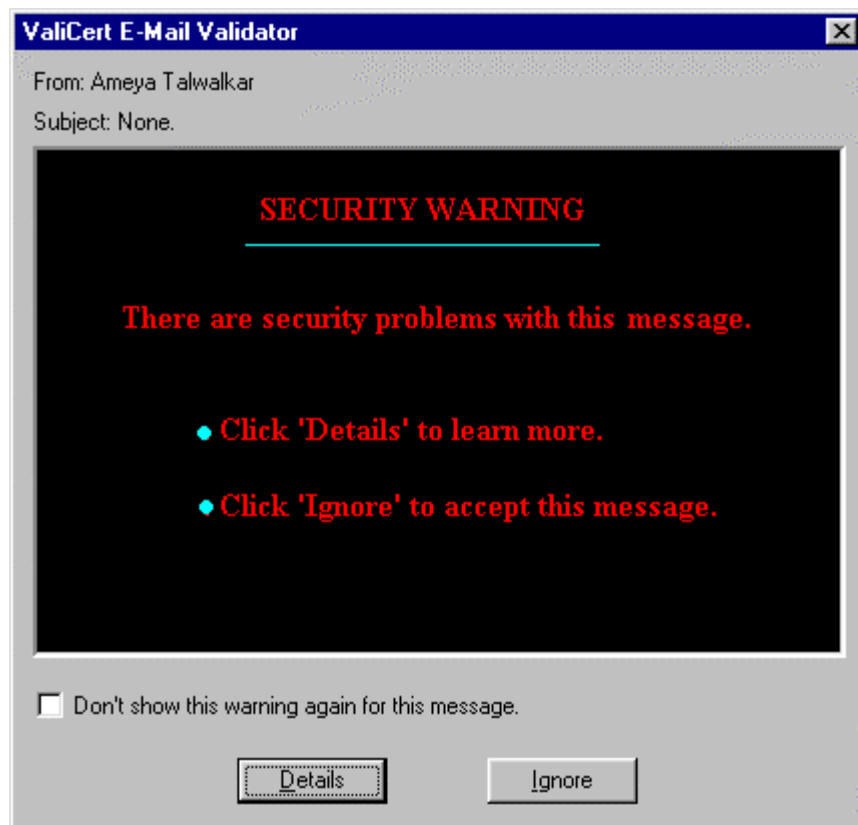
Certificate Status Message: Server-Based Applications



Message Options:

- Certificate Has Been Revoked (illustrated above)
- Validation Response Has Expired
- Validation Response Is Not Activated
- Certificate Issuer Is Not Trusted by the VA
- Validation Issuer Is Not Trusted
- Certificate Chain Could Not Be Constructed
- Cannot Connect to the Validation Authority

Certificate Status Message 1A: Client-Based Applications



Certificate Status Message 1B: Client-Based Applications

ValiCert E-Mail Validator [X]

Mail Information

Mail from: Ameya Talwalkar

Sender's E-Mail: ameyat@valicert.com

Subject: None.

Mail delivery on: Tue, 15 Dec 1998 14:35:18

Certificate Information

Serial No: 248C56BD00000017

Issuer: US, CA, Mt. View, Valicert, SQA, Testlab8CA


Security Problem

This message is signed with a 'Revoked' certificate.

Actions

Certificate Status Message 2: Client-Based Applications

ValiCert E-Mail Validator : Unverified Message [X]

 The Digital ID used to sign this message could be validated using the ValiCert Validation Resource.
See the documentation for more information.

☐ Don't warn me again for this message

Certificate Status Message 3: Client-Based Applications

