

Securing a Web Server on NetWare

To meet today's strident security requirements, companies want to secure content stored on web servers. The best way to secure this content on web servers that run on the NetWare platform is to use a Secure Sockets Layer (SSL) certificate, which allows a web server and a web browser client to encrypt the data they exchange.

To enable SSL encryption on the web server, you must have an SSL server certificate. NetWare 6 and NetWare 5.1 include the components necessary to generate an SSL server certificate. There's a wrinkle, however; most web browsers will seamlessly integrate only with SSL server certificates that are created by a handful of intermediate certificate authorities (CAs) that are preregistered within the browser itself.

Because the SSL server certificate cannot be verified by an intermediate CA, each time a user logs in to your company's web site, that user is prompted to accept the SSL server certificate for the current session. The only way to get around this requirement is to have users manually import the SSL server certificate into their browser. This solution is problematic and a training issue for users. A better solution is to implement an SSL server certificate from an intermediate CA such as VeriSign.

This article explains all of the steps that I took to help a customer implement a VeriSign 128-bit SSL server certificate. However, the steps outlined in this document also apply if you are using a 40-bit SSL server certificate.

The customer mentioned in this article is using Novell eDirectory, NetWare 5.1 with Support Pack 4, and Netscape Enterprise Server. Your environment may be different. For example, you may be implementing a different vendor's certificate, or you may be using Apache web server on a NetWare 6 server. Despite these differences almost every step outlined in this article will also apply to you. Of course, configuring the web server to use the certificate will be different, depending on the web server and the version of the web server you are using.

Note. Any updates or improvements to this article will be appended to the Novell Support Connection Technical Information Document (TID), which you can access at <http://support.novell.com/cgi-bin/search/searchtid.cgi?/10074010.htm>.

In a nutshell, you must complete the following steps to implement a certificate from an intermediate CA:

1. Create a new Key Material object in the eDirectory/NDS tree.



2. Export information from the Key Material object. This information is called a *Certificate Signing Request or CSR*.
3. Send the CSR, which is just an ASCII text file, to VeriSign.
4. VeriSign will send you a Certificate Key, which is just a bunch of ASCII characters.
5. Import the Certificate Key from VeriSign into the Key Material object you created in the eDirectory/NDS tree.
6. Enable SSL on your web server, and tell it to use the Key Material object in the eDirectory/NDS tree into which you imported the Certificate Key.

PREREQUISITES

Before you begin to complete these steps, you should complete the following prerequisites:

Certificate Vendor

Visit the web site of the certificate vendor you have selected, and learn how to work with that certificate vendor. Because VeriSign is the most popular certificate vendor, this article has a VeriSign slant. No matter which vendor you choose, however, the steps outlined in this article will still be relevant.

My customer and I discovered the following information for VeriSign certificates. If you are implementing a 40-bit SSL certificate, tell VeriSign you want a Novell certificate. If you are implementing a 128-bit SSL certificate for Netscape Enterprise Server on NetWare, tell VeriSign you want a Netscape/iPlanet certificate.

You may find the following information helpful in dealing with VeriSign. The VeriSign Customer Support department is open 5 a.m. to 6 p.m. Pacific Standard Time Monday through Friday. You can e-mail the VeriSign Customer Support department at support@verisign.com, and you can visit the VeriSign web site at www.verisign.com. VeriSign's telephone number is

877-GET-VRSN (877-438-8776) or 650-426-3400.

Before you attempt to create a CSR (which is discussed later in this article), make sure that you understand how your particular certificate vendor wants you to positively identify the server on which the certificate will be used. For example, with VeriSign, you may need to use a D-U-N-S number, or you need to agree on another way to positively identify your company to VeriSign. (The D-U-N-S number is discussed later in this article.)

Server

If you are going to use a 128-bit SSL server certificate, you must use the latest Public Key Infrastructure (PKI) and Novell International Cryptographic Infrastructure (NICI) software components. Any revision of the NetWare 6 server platform includes these software components. For NetWare 5.1, you must be using eDirectory 8.6 or above.

If you are going to use a 40-bit SSL server certificate, any version of the PKI or NICI server software will probably work. You may use a 40-bit SSL server certificate if you do not have eDirectory 8.6 or later implemented on NetWare 5.1

Workstation

You need the latest PKI snap-ins for ConsoleOne and the latest NICI software installed on your workstation. When you perform the steps outlined in this article, you must be using the workstation on which you have installed the ConsoleOne snap-ins and NICI software.

To install these snap-ins and the latest NICI software, complete the following steps:

1. Go to <http://download.novell.com>.
2. Download the latest PKI snap-ins for ConsoleOne by selecting Certificate Server as the product, Windows 2000 as the platform, <All Dates> as the date, and English as the language. At the time this article was written, the PKI software was called *2.21 Snap-in on Windows 95/98/NT/2000*.
3. This software does not have a README file or an install routine. Complete the following steps to install this software:
 - a. Run the UNZIP utility to expand the compressed file.
 - b. When prompted for a path to expand the software, indicate the path to



Figure 1. When you save the CSR, you should save it in Base 64 format.

4. Return to <http://download.novell.com>.
5. Download NICI for Windows by selecting Novell International Cryptographic Infrastructure as the product, Windows 2000 as the platform, <All Dates> as the date, and English as the language. At the time this article was written, the software was called *2.4 on Windows 95/98/NT/2000*.
6. Run the *.EXE that you downloaded, and follow the installation wizard. This software, which is necessary for the Novell Certificate Server Snap-in to work, will be installed on the machine from which you will run ConsoleOne.

CREATING A KEY MATERIAL OBJECT AND GENERATING A CSR

To create a Key Material object and to generate a CSR, complete the following steps:

1. From ConsoleOne, access the eDirectory/NDS tree that contains the NetWare server on which Netscape Enterprise Server (or Apache) is running.
2. Highlight the Organizational Unit (OU) that holds the NetWare server running the web server, right-click, and select New Object > NDSPKI:Key-Material.

Note. If you receive the error “No creator snapins,” you are lacking the PKI snap-ins needed to create the NDSPKI:KeyMaterial. Make sure you have completed the workstation prerequisites mentioned earlier.
3. Specify the NetWare server on which the Netscape Enterprise Server (or Apache) is running. Enter a name for

the certificate, such as <webserver> certificate.

4. Choose the Custom creation method, and click Next.
5. Select External Certificate Authority, and click Next.
6. Specify the RSA Key Size. Usually, you will just keep the default size of 2048. Also place a check by the box that says Allow Private Key to be Exported, and click Next.
7. On the next page, edit the Subject name field. Understanding the syntax of this field isn't really straightforward. You should read the note about the D-U-N-S number and also look at the example for the State of Hawaii. The syntax is as follows:

```
.CN=<The server's publicly known DNS name>
.OU=<The OU that holds the NetWare server
on which the Netscape Enterprise Server
runs>.OU=<The OU above the previous OU (if
there is one). Keep adding OUs until you reach
the Organization (O) level>.O=<D-U-N-S
number, which is explained below>.L=<The
city this server is in. (L stands for loca-
tion.)>.S=<The state the server is in>.C=<The
country>
```

Note. A D-U-N-S number is how your organization is registered at Dun & Bradstreet to positively identify your organization in the marketplace. Dun & Bradstreet is a credit-rating firm that helps companies know how well another company is able to pay its bills. VeriSign uses an organization's D-U-N-S number to guarantee authenticity and uniqueness.

Because Dun & Bradstreet has uniquely identified 64 million organiza-



Figure 2. One of the steps you must complete is importing the certificate.

Dun & Bradstreet database, thereby avoiding extra work. VeriSign requires the D-U-N-S number identifier for its high-end 128-bit keys. If you cannot provide a D-U-N-S number, contact VeriSign to find another way to positively identify your organization. As you see in the example below, the organization in this article has a D-U-N-S number of HAWAII, STATE OF

```
.CN=GWWEB.STATE.HI.US.OU=WEBACC
.O=HAWAII, STATE OF.L=
HONOLULU.S=HAWAII.C=US
```

8. Click OK.
9. For the Signature Algorithm, use SHA1/RSA, the standard recommended by Novell, and then click Next.
10. Review the information in the Summary screen to make sure that it is correct, and click Finish.
11. When the next screen appears, click Save to save the CSR as a file in the Base 64 format. (See Figure 1 on p. 27.) This is the CSR that you send to VeriSign. The file will have a *.B64 file extension.
12. After receiving your CSR, VeriSign generates a certificate key and sends you a message, like the one below:

Dear VeriSign Global Server ID Customer,
 Congratulations! Your official Global Server ID is included at the end of this message. For installation instructions for your Server ID, please refer to <http://www.verisign.com/support/install/index.html>.

Thank you for your business and interest in VeriSign products!

```
-----BEGIN CERTIFICATE-----
A WHOLE BUNCH OF CHARACTERS
-----END CERTIFICATE-----
```

IMPORTING THE CERTIFICATE

You will need to use Internet Explorer 5.5 or above when completing the steps for importing the certificate. This article was written based upon testing with Internet Explorer 5.5 and Internet Explorer 6.0.

To prepare the certificate key for importing, complete the following steps:

1. Copy the entire certificate key from the e-mail you received from VeriSign to the Windows clipboard. Be sure to include -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----. However, do not include any extra characters or even spaces.
2. Paste the VeriSign certificate key to a new Notepad file. Save the file with the .CER extension. The name of the file does not matter; it just must have the extension *.CER .
3. From Windows Explorer (not Internet Explorer), double click on the *.CER file that you just created. A dialog box appears, showing the certificate information for this certificate.

Click the Install Certificate button shown in Figure 2. This will launch the Import wizard. Select the Next button. Keep all defaults, and then click the Finish button. After the Import Successful dialog box appears, click OK.

4. Run Internet Explorer from the same computer on which you imported the *.CER file in Step 3. Select Tools | Internet Options | Content | Certificates, and then select the Other People tab. Highlight the Certificate that you just imported, and select Export | Next | Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B). Also select the check box for Include All Certificates in the Certification Path if Possible.

Click the Next button. Enter a path and name to the file, without specifying a file extension. (The name of the file doesn't matter.) Select the Next button. Select the Finish button.

To import the certificate key, complete the following steps:

1. Run ConsoleOne.

2. Edit the Key Material object that you created earlier.
3. Access the Certificates property page, and select the Public Key Certificate page.
4. Click the Import button.
5. In the first page that comes up in the Import wizard, select the check box for No Trusted Root Certificate Available. Click the Next button.
6. In the next page of the Import wizard, click the Read from File button. Change the Files of Type drop-down to list *.P7B files. Browse to the *.P7B file that you exported previously from Internet Explorer.

Tip. When you select this file, you will see a little square block in the next screen. Do not try to delete the block; it's just fine.

7. Click the Finish button.

Note. If you receive a - 601 error at this point, you probably do not have an eDirectory/NDS replica on the server for which you are trying to import the certificate. The replica should be the same replica in which the NetWare server, which is running your Netscape Enterprise web server, is located.

8. When the screen with the Validate button appears, select Validate. In the Public Key Certificate screen, note that you can select only Cancel, but the certificate was imported.

ENABLING SSL ON NETSCAPE ENTERPRISE

You have imported the certificate into eDirectory/NDS. Next, you need to enable SSL on your server and specify that the web server should use the SSL certificate you imported. To enable the SSL certificate on Netscape Enterprise Server, complete the following steps:

1. Edit the MAGNUS.CONF file for the Netscape Enterprise Server. You will generally find this file in the following location:

```
SYS: NOVONYX\SUITESPOT\HTTPS-
<FILE SERVER NAME>\CONFIG
```

2. Add the following lines at the end of the MAGNUS.CONF file:

```
Certfile SSL <Name of the Key Material object in
eDirectory>
Keyfile SSL <Name of the Key Material object in
eDirectory>
```

Note. The certificate name portion of this command is case sensitive.

Also, the name of the Key Material object should not include the dash and the servername. For example, if in ConsoleOne the name of your Key Material object is GWWEB-Hawaii - HISERVER1, your command should not include the - HISERVER1. You should enter the following command:

```
Certfile GWWEB-Hawaii
Keyfile GWWEB-Hawaii
```

You may notice that the Certfile and Keyfile lines already exist, with reference to SSL Certificate DNS or something else. Remove these two lines, or comment them out with a pound symbol.

3. Unload your Netscape Enterprise Server, and reload it. The server should now allow SSL connections. Access the web server in the following manner:

```
https://<web server name>
```

If you try to access your web server via its IP address instead of its DNS name, you may be prompted to accept the certificate for your web server. Veri-Sign generated the certificate key for your server only when it is accessed via its DNS name.

ENABLING SSL ON APACHE WEB SERVER

To enable SSL on an Apache web server, you need to enable four lines in the Apache server's configuration file. Usually the name of this configuration file is ADMINSECV.CONF, which is located in the SYS:APACHE\CONF directory.

The ADMINSECV.CONF file probably already contains these lines. You will just need to change the certificate name which is in the double quotes on the "SecureListen" line.

If you are using GroupWise 6 WebAccess with Apache and you start APACHE with the GWWEBUP.NCF file, you need to add these four lines to the top of the SYS:\APACHE\CONF\GWAPACHE.CONF file.

To add these four lines, complete the following steps:

1. Edit the appropriate *.CONF file.

2. Add or modify the four lines as shown below.

```
LoadModule tls_module modules/
    mod_tls.nlm
<IfModule mod_tls.c>
SecureListen <web server IP address>:443
    "<Name of the Key Material object in
    eDirectory>"
</IfModule>
```

Note. The name of the Key Material object is case sensitive. Also, the name you enter should not include the dash and the servername. For example, if in ConsoleOne the name of your Key Material object is: GWWEB-Hawaii - HISERVER1, your statement should not include - HISERVER1, as the following example shows:

```
LoadModule tls_module modules/
    mod_tls.nlm
<IfModule mod_tls.c>
SecureListen 166.122.101.5:443 "GWWEB-
    Hawaii"
</IfModule>
```

3. Unload the Apache web server, and reload it. It should now allow SSL connections. Access the web server in the following manner: `https://<web server name>`.

TESTING METHODS AND TROUBLESHOOTING

When I devised the steps for implementing an SSL server certificate, I was working in a live customer environment. The web server that I was enabling the SSL certificate for was supporting GroupWise WebAccess users. Bringing down the web server required an outage notification and lead time. I needed to test whether or not this certificate was working without bringing down the web server.

I found you can test the certificate with the iMonitor/NetWare Management Portal, which runs on the NetWare server. The iMonitor/NetWare Management Portal is really just a special-purpose web server which listens at port 8008. Bringing down this iMonitor web server has no impact on the other web server loaded on the NetWare server. To test an SSL certificate with the iMonitor/NetWare Management Portal, complete the following steps:

1. At the console prompt of the NetWare server, unload HTTPSTK (which also unloads PORTAL.NLM and NDSIMON.NLM).
2. Now reload HTTPSTK with the following syntax:

```
HTTPSTK.NLM /SSL /keyfile:"<Name of the
    Key Material object in eDirectory>"
```

Note. The certificate name portion of this command is case sensitive. Also, the name of the Key Material object you enter should not include the dash and the servername. For example, if in ConsoleOne the name of your Key Material object is GWWEB-Hawaii - HISERVER1, your command should not include - HISERVER1. Instead, you should enter the following command:

```
HTTPSTK.NLM /SSL /keyfile:"GWWEB-
    Hawaii"
```

3. Load NDSIMON.
4. Load PORTAL.
5. Access your web server at port 8008, which is the default port for iMonitor. To do so, use the following syntax:

```
http://<web server DNS name>:8008
```

For example, you would enter the following:

```
http://gwweb.state.hi.us:8008
```

When you access this URL, you will be prompted to log in to iMonitor/NetWare Management Portal.

Try to log in, and determine if you have a secure session by clicking the Lock icon in Internet Explorer or the Key icon in Netscape at the bottom part of your browser and viewing the certificate details. You should be able to see that you are using the certificate you imported. If this works, you have confirmed that certificate should also work in your web server.

Tay Kratzer works for Novell as a primary support engineer for three of Novell's large accounts. Tay is the author of Novell's GroupWise 6 Administrator's Guide, and coauthor of GroupWise 6 Upgrade Guide, and GroupWise WebAccess & Wireless User's Guide, which are available at www.caledonia.net. ●