

We recommend you bookmark this FAQ document

NOTE: this FAQ document is specific to DNS Assurance Services. For general information regarding Digital Certificates, please refer to the Help button on the Digital ID Center page.

Contents

1	What benefits do VeriSign Digital Certificates provide?.....	2
2	Do Digital Certificates apply to all DNS Manager users?.....	2
3	Is there a fee for VeriSign Digital Certificates?.....	2
4	How do I Enroll for my VeriSign Digital Certificate?.....	2
5	What if I'm a Regular User and need to be changed to a Master User?	6
6	When trying to Enroll, what if I get an error message regarding Active X?.....	6
7	How do I know if the Digital Certificate is on my machine, and which is the correct one?	7
8	Does my Digital Certificate expire?.....	8
9	How do I check the expiration date of my Digital Certificate?	8
10	What happens if I don't renew my Digital Certificate before it expires?	8
11	How do I install Digital Certificates on multiple machines?	8
12	In the DNS Manager, why do I get the Error message: "certificate is invalid"?	10
13	What if my e-mail address changes?	10
14	What if a user leaves the company?	11
15	What happens to the Digital Certificate when a User is deleted from the DNS Manager?....	11

1 What benefits do VeriSign Digital Certificates provide?

VeriSign Digital Certificates provide you added security in accessing the DNS Manager tool by supporting two-factor authentication: 1) verification that a valid DNS Assurance Services certificate is provided, and 2) verifying that a valid user name and password is provided. Users must have a valid certificate in order to get to the DNS Manager logon page.

2 Do Digital Certificates apply to all DNS Manager users?

Yes. The DNS Manager tool accommodates 3 user types: master, regular, and read-only. All user types will be issued a Digital Certificate as soon as they are added to the DNS Manager tool.

The initial Master User is established upon account creation (by CSR). The initial Master User can create additional Master Users for their Account. Any Master User can Add/Edit/Delete Regular or Read-only Users. Each User will automatically be sent an email containing a temporary password, a link to the Digital Certificate enrollment website and a PIN code to obtain a Digital Certificate.

Master Users ARE RESPONSIBLE FOR DELETING USERS WHO HAVE LEFT THE COMPANY, from the DNS Manager tool.

3 Is there a fee for VeriSign Digital Certificates?

No. VeriSign Digital Certificates are provided at no additional cost for DNS Assurance Services customers.

4 How do I Enroll for my VeriSign Digital Certificate?

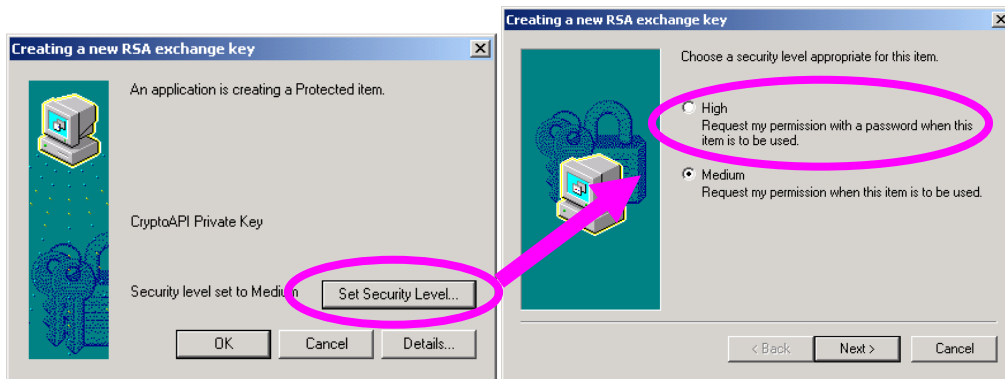
Once you have been added as a User of the DNS Manager, you will receive an automated e-mail with your temporary password, a link to the Digital Certificate enrollment web site (<https://certificates.dnsassurance.com/enrollment/>) and a PIN code to obtain your Digital Certificate. Your Logon Name is not included in this email for security purposes*; however, you will need to know your Logon Name, and have your PIN code in order to enroll for your certificate as illustrated in the screenshots below.

* If you cannot remember your Logon Name, you may contact your Account's Master User(s) or VeriSign Customer Service (dnssupport@verisign-grs.com or 703-925-6999).

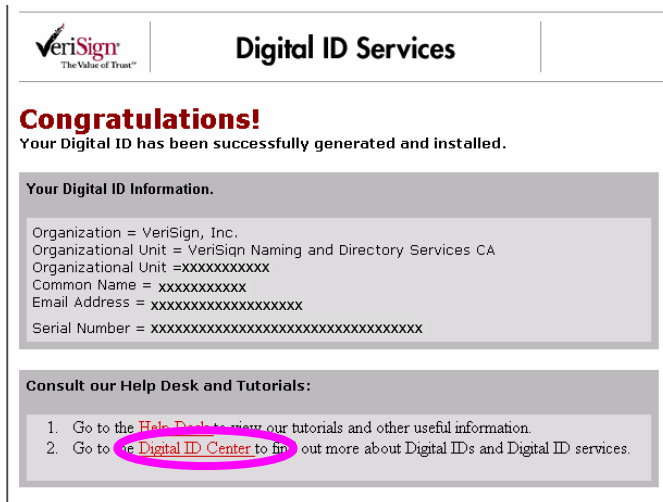
1. Begin the Enrollment steps as illustrated below, and click Accept.

The image displays two screenshots from the VeriSign Digital ID Center website. The left screenshot shows the 'VeriSign DNS Assurance Services' menu with three options: 'ENROLL', 'RENEW', and 'INSTALL CA'. The 'ENROLL' option is circled in pink, and a pink arrow points from it to the right. The right screenshot shows the 'Enrollment' page with a 'Complete Enrollment Form'. The form includes fields for 'user-logout name' and 'Enter PIN:'. Below the form is an 'Accept' button and a 'Cancel' button.

2. Next, if you are using Microsoft, you will receive the following pop-ups. Click the Set Security Level button and change the setting to High. This protects your private key with a password, so that upon logging on to the DNS Manager, you will also need to enter the password.

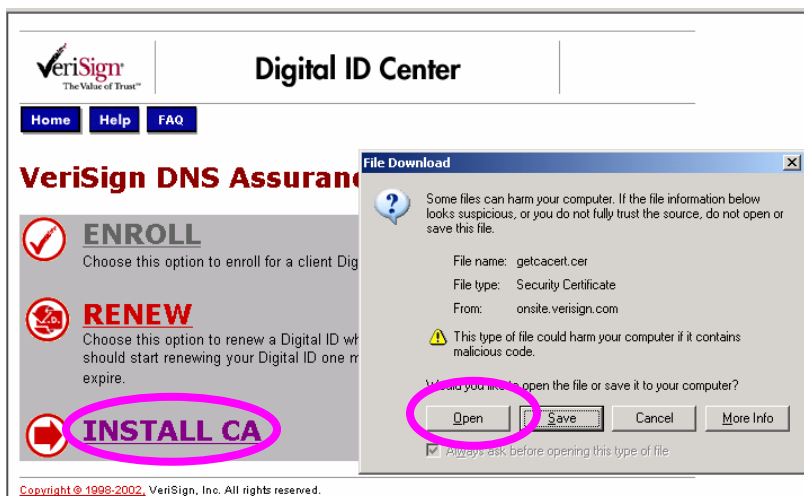


3. Upon successful Enrollment, you will then see the Congratulations page.

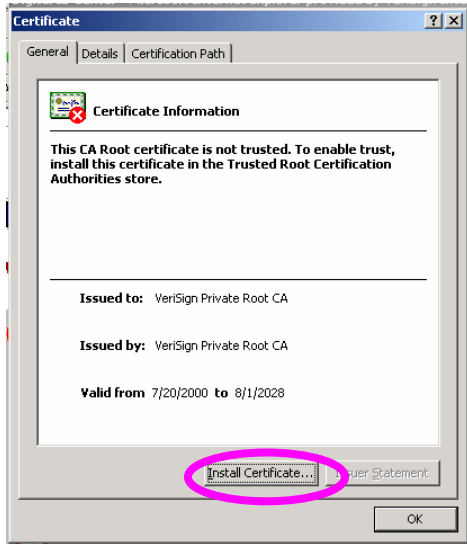


4. Click on the Digital ID Center link at the bottom of the Congratulations page.

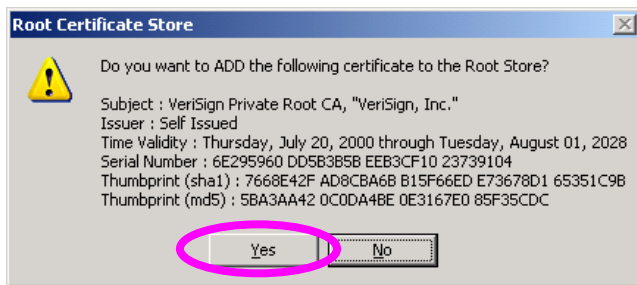
5. In the Digital ID Center page, click the Install CA link. In the File Download pop-up screen, click Open.



6. Click the Install Certificate button. In the subsequent prompts, click Next → Next → Finish

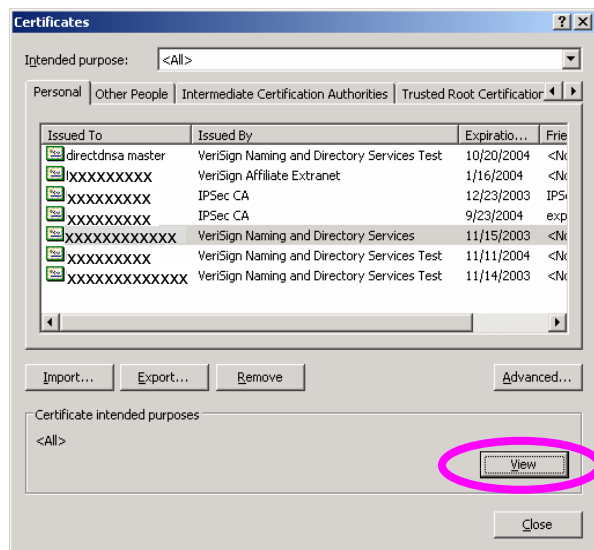


7. Then click Yes to add the certificate to the Root Certificate Store



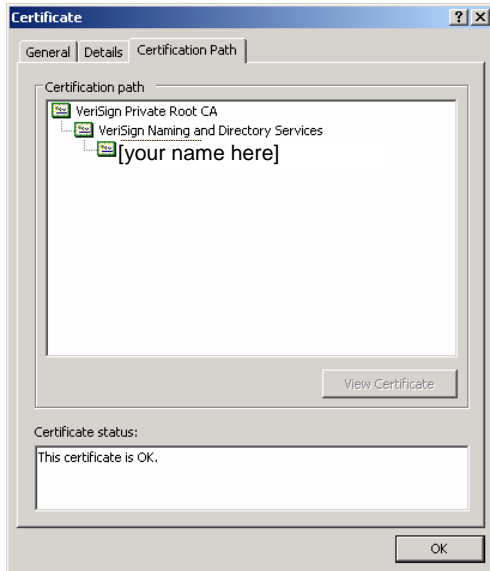
8. You will receive confirmation that the Import was Successful. Click OK

9. To verify, click the Tools drop-down menu → Internet Options → Content → Certificates. Select the cert you just installed (Issued By VeriSign Naming and Directory Services). Click View.

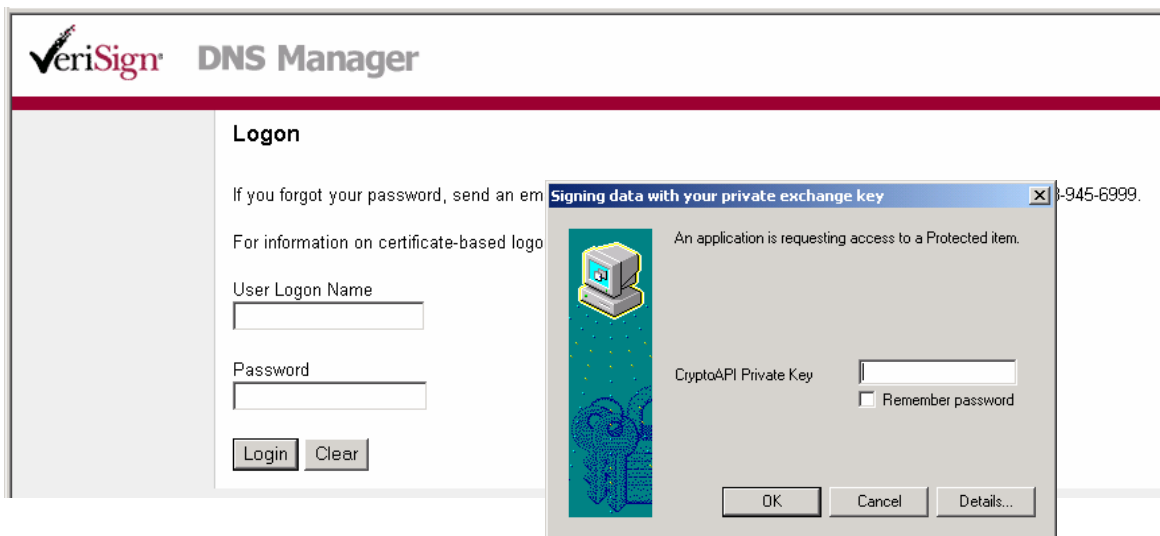


10. Click the Certification Path tab. Ensure that your Certificate is listed under the VeriSign Private Root CA, and VeriSign Naming and Directory Services hierarchy as illustrated below. This provides confirmation of your certificate's validity so that your browser trusts the root that issued it.

Click OK → Close → OK



11. You can now logon to the DNS Manager: www.dnsassurance.com. You will first be prompted to select the appropriate Certificate, then click OK. Next, you will be prompted to provide the password that you created for the High Security Level protection of your Private Key during your Enrollment. After entering your password, click OK.



You can then enter your Logon Name and Password* for the DNS Manager and begin managing your DNS.

* If you were already an existing user upon v2.0 launch (Nov.13, 2003), then this password for the DNS Manager is the same as it was prior to the launch. If you are a new User added to your Account in the DNS Manager after the v2.0 launch, then your use the temporary password as provided in the email you received after you were added as a User.

Note: You may be prompted to select the appropriate Certificate and prompted for your security password upon subsequent sessions when accessing the DNS Manager.

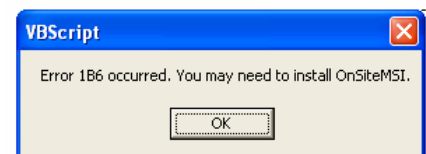
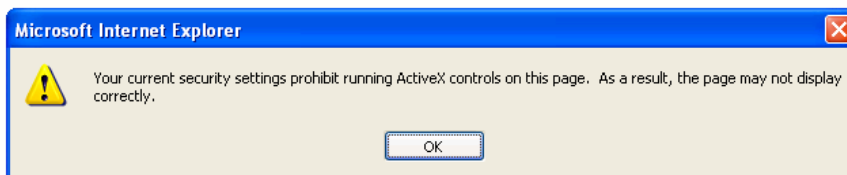
5 What if I'm a Regular User and need to be changed to a Master User?

If you need to change your User Type, you need to be re-created as a new User with the different User Type a new Logon Name; you will be issued a new certificate. This can be done either by a Master User for your Account, or by VeriSign Customer Service (dnssupport@verisign-grs.com or 703-925-6999), to perform the following steps:

- 1) First, the existing Master User/VeriSign CSR needs to Add you into the DNS Manager as the new User Type, with a new Logon Name.
- 2) You will automatically receive an email that includes a new PIN, and a temporary password for the DNS Manager.
- 3) Go to the Enrollment page, and follow the steps as outlined in FAQ #4 above.
- 4) You should then remove your old Certificate for your previous Regular User Type, to avoid confusion as to which is the correct certificate when logging on to the DNS Manager as Master User. Go to the Tools drop-down menu → Internet Options → Content tab → Certificates button. In this window, find the certificates Issued By "VeriSign Naming and Directory Services." Check the listed expiration dates to identify your old certificate, and click the Remove button.
- 5) Then close your browser and re-open it. Go to the DNS Manager: www.dnsassurance.com where you will be prompted to identify the certificate before you can logon to the DNS Manager using your new Master User Logon Name and Password.
- 6) Go to the Manage Users tab, and delete your previous Regular User entry.

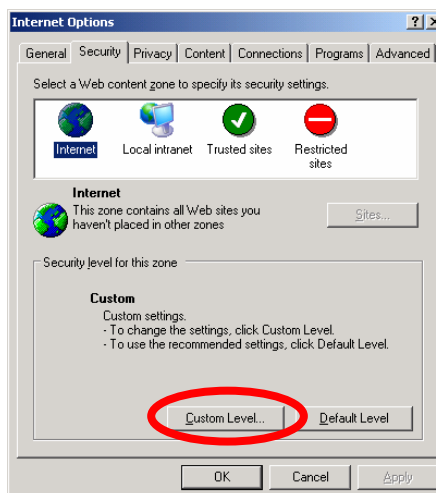
6 When trying to Enroll, what if I get an error message regarding Active X?

If you experience problems enrolling for your Digital Certificate, such as one of the following error messages, it might be that Active X controls are not enabled:

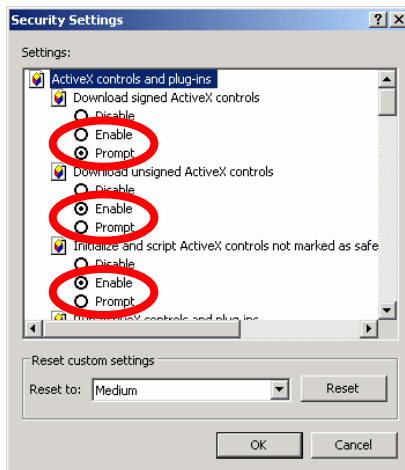


Digital Certificates use ActiveX controls to streamline and automate functions in the certificate lifecycle. Your browser settings may prevent you from installing ActiveX controls, thereby preventing you from enrolling for certificates or viewing other Web pages.

- 1) First, check your Active X control settings in the Tools drop-down menu → Internet Options → Security tab → Custom Level button. NOTE: if this button section is grayed out, then you do not have permission to change your Active X controls. Go to Step (3).



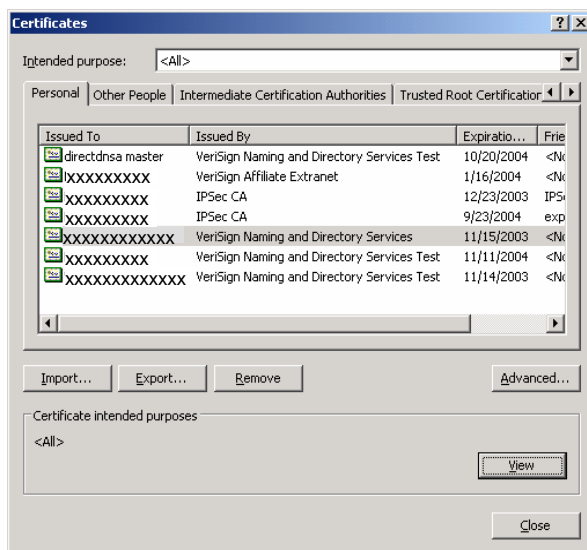
- 2) Check if the 5 entries under the “Active X controls and plug-ins” section have Disable selected. If so, change the selection to either Enable or Prompt for all 5 entries and go to Step (4). NOTE: if this section is grayed out, then you do not have permission to change your Active X controls → continue to Step (3).



- 3) Contact your IT Administrator/Help Desk to have Active X enabled on your machine [by performing Step (2)]. You can then complete the Enrollment process for your VeriSign Digital Certificate → go to Step (5). If your IT policies are such that Active X cannot be enabled on your machine, continue to Step (4).
- 4) If Active X controls cannot be changed in your browser, another method to get the ActiveX control files required for Digital Certificates into your browser is to use VeriSign’s OnSiteMSI package which delivers all the necessary files. To do this, contact VeriSign Customer Service (dnssupport@verisign-grs.com or 703-925-6999) to have them email you the OnSiteMSI ActiveX control package. Upon installing OnSite MSI, you can then complete the certificate Enrollment.
- 5) Note that this same procedure will have to be followed upon Renewal of your certificate.

7 How do I know if the Digital Certificate is on my machine, and which is the correct one?

To check for your Digital Certificate, go to the Tools drop-down menu → Internet Options → Content tab → Certificates button. Find a certificate Issued By “VeriSign Naming and Directory Services.” If you have more than one certificate Issued By this entity, check the listed expiration dates. For any certificates that you no longer need, you can click the Remove button.

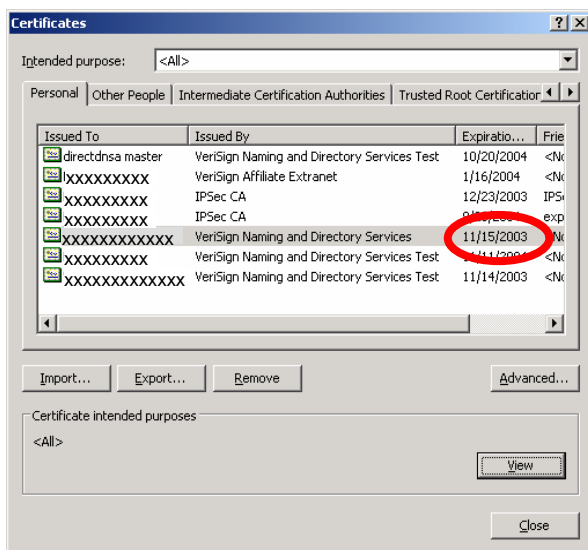


8 Does my Digital Certificate expire?

Yes. Digital Certificates are valid for 1 year from date of Enrollment. YOU ARE RESPONSIBLE FOR RENEWING YOUR CERTIFICATE. As a courtesy, you will receive an e-mail notification 30 days prior to your certificate expiration date as a reminder to renew, and instructions for doing so. You can renew your certificate anytime within 30 days of your expiration date, via the Digital ID Center page: <https://certificates.dnsassurance.com/enrollment>.

9 How do I check the expiration date of my Digital Certificate?

To check the expiration date of your Digital Certificate, go to the Tools drop-down menu → Internet Options → Content tab → Certificates button. In this window, look for digital certificates Issued By “VeriSign Naming and Directory Services” and check the listed expiration date.



10 What happens if I don't renew my Digital Certificate before it expires?

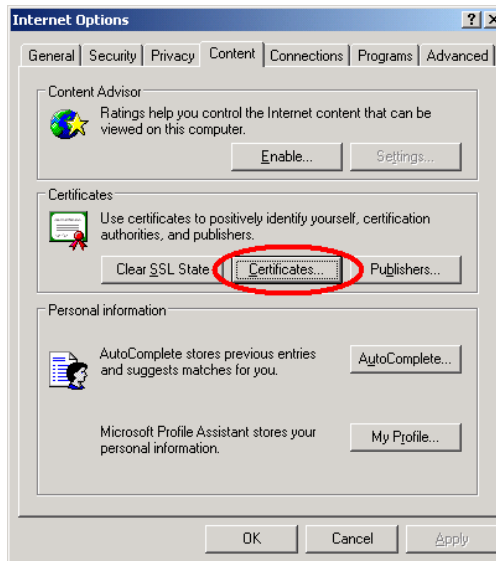
It is YOUR RESPONSIBILITY TO RENEW your Digital Certificate prior to expiration (note that there is no cost to renew). If you fail to do so, you will be deleted as a User from the DNS Manager, your certificate will be revoked, and you will be unable to logon.

To regain access to the DNS Manager, a Master User will have to add you again as a user with a new Logon Name, and a new certificate will be issued. If you were your Account's only Master User, then you need to contact VeriSign Customer Service (dnsupport@verisign-grs.com or 703-925-6999) to re-add you as a user with a new Logon Name, and a new certificate.

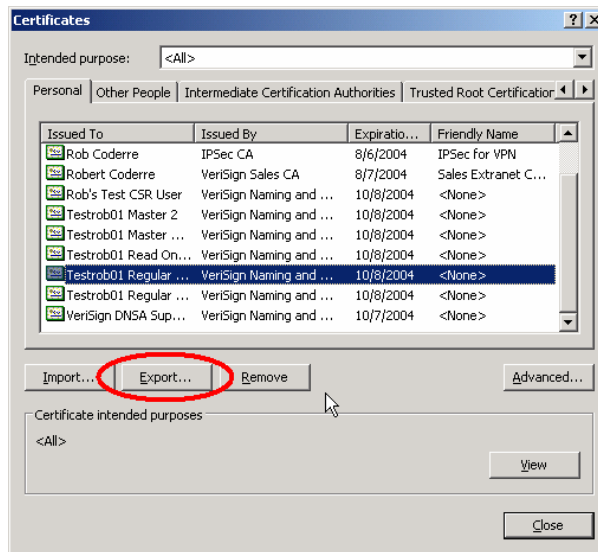
11 How do I install Digital Certificates on multiple machines?

These instructions are valid for Internet Explorer. If you use another browser, the process is similar, but some of the steps may be different. To export a Digital Certificate and install it on another machine do the following:

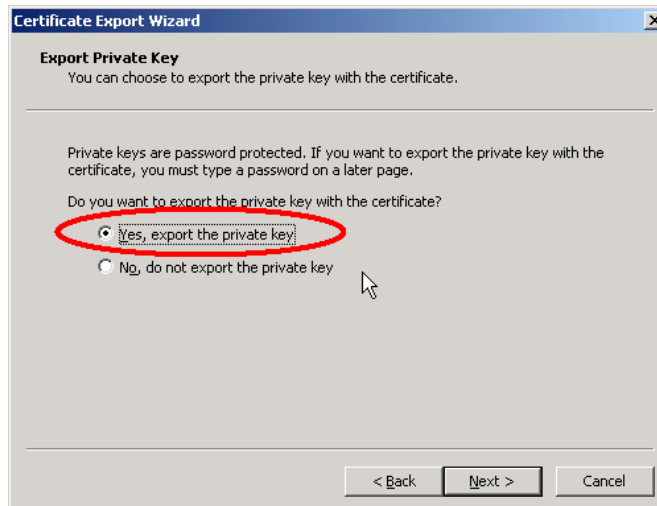
1. Go to the Tools drop-down menu → Internet Options → Content tab → Certificates button.



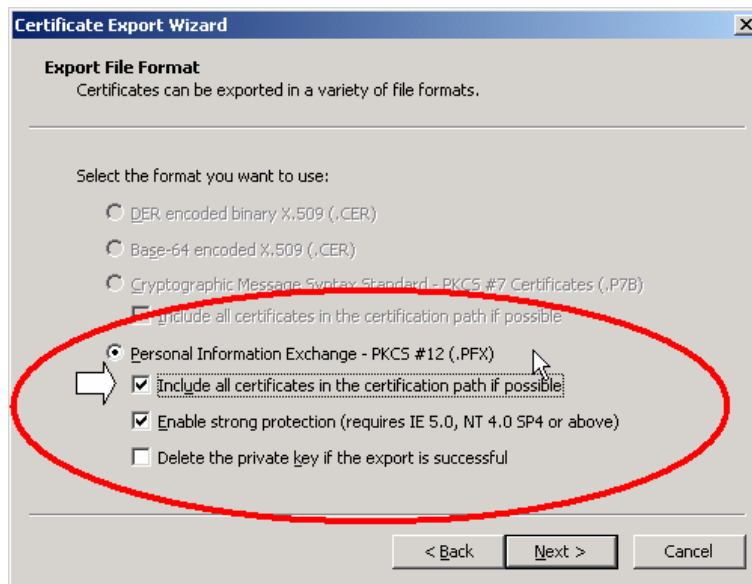
2. Select the Digital Certificate from the list that you want to export and click on "Export".



3. Follow the instructions in the Certificate Export Wizard. When prompted, select "Yes, export the private key". THIS IS CRITICAL!



- Next, select “Personal Information Exchange – PKCS #12” and check the box for “Include all certificates in the certification path, if possible”. This ensures that the root CA certificate is included in the export file.



- Enter a password to protect the private key (optional, but recommended), select a filename and click on Finish to complete the export process.
- Copy the resulting PFX file to the new machine. Double-click the file and run Certificate Import Wizard.
- Enter the password you specified during the export and select the appropriate options for key protection and export capability (both recommended). The system will choose the certificate store; then click Finish.
- Repeat as necessary for different machines.

12 In the DNS Manager, why do I get the Error message: “certificate is invalid”?

If you receive this message upon attempting to logon to the DNS Manager, it means that the User Logon Name/Password that you entered does not match the Digital Certificate presented in your browser.

If you have multiple certificates installed on your machine* you may need to close your browser and re-open it, select the appropriate certificate and try again.

* In Internet Explorer, check the Tools drop-down menu → Internet Options → Content tab → Certificates button, to ensure it includes a certificate for your name Issued By: VeriSign Naming and Directory Services.

If you are unable to locate your Digital Certificate, a Master User can add you again as a user with a new Logon Name (a new certificate will be issued to you) and delete your previous Logon Name entry. If you are the only Master User in your Account, then you need to contact VeriSign Customer Service (dnssupport@verisign-grs.com or 703-925-6999) to re-add you as a user with a new Logon Name (a new certificate will be issued), and delete your previous Logon Name entry.

13 What if my e-mail address changes?

If your e-mail address changes after you have obtained a Digital Certificate, you will need to be re-created as a user with a new Logon Name, and obtain a new certificate. A Master User for your Account can create you as a new user, and delete your previous Logon Name entry.

If you are a Master User, and there are no other Master Users in your Account, then you need to contact VeriSign Customer Service (dnssupport@verisign-grs.com or 703-925-6999) in order to have them create you as a new user (a new certificate will be issued), and delete your previous Logon Name entry.

14 What if a user leaves the company?

If any of your Account's users leave your company, the ACCOUNT'S MASTER USERS ARE RESPONSIBLE for deleting that user from the DNS Manager tool. Once a user is deleted from the DNS Manager, that user's Digital Certificate will also be revoked.

If you are your Account's only Master User and you leave the company, you need to create another Master User, then have that user delete you – or you can contact VeriSign Customer Service (dnssupport@verisign-grs.com or 703-925-6999).

When a user is "deleted" (i.e., Status is changed to Inactive), then another user cannot be added with the same Logon Name.

15 What happens to the Digital Certificate when a User is deleted from the DNS Manager?

If you are deleted as a User from the DNS Manager, your Digital Certificate will also be automatically revoked. Your prior Logon Name cannot be re-used; this is for audit purposes. To be re-established as a User, a Master User will have to Add you again as a User with a new Logon Name, and you will need to obtain a new certificate.

If any of your Account's users leave your company, YOUR ACCOUNT'S MASTER USER(S) IS RESPONSIBLE for deleting that user from the DNS Manager tool.