Wavecrest®InstallationGuide



Wavecrest Certificate SHA-512

www.wavecrest.net

Copyright

Copyright © 1996-2018, Wavecrest Computing, Inc. All rights reserved. Use of this product and this manual is subject to license. Information in this document is subject to change without notice. 904 East New Haven Avenue, Melbourne, FL 32901 USA www.wavecrest.net

Trademarks

The following are trademarks, registered trademarks, or service marks of Wavecrest Computing, Inc.: Wavecrest Computing, Inc., CyBlock[®] App, CyBlock[®] Appliance, CyBlock[®] Client, CyBlock[®] Cloud, CyBlock[®] Directory Agent, CyBlock[®] ISA, CyBlock[®] Software, Cyfin[®], and OtherWise[™]. All other trademarks mentioned are the property of their respective owners.

Downloading the Wavecrest Certificate

- Contact Technical Support at (321) 953-5351, Ext. 4 or <u>support@wavecrest.net</u> for the link to the certificate file and download it.
- Note the location of the downloaded file (nokeywavecrest.crt) as it will be needed when installing the Wavecrest Certificate.

Installing the Wavecrest Certificate Using Microsoft Internet Explorer 11/Google Chrome 64

NOTE: The Chrome browser uses the same certificate settings as Internet Explorer.

- 1. Open your Internet Explorer or Chrome browser.
- 2. Continue with one of the following:
 - In Internet Explorer, from the Tools menu, click Internet options.
 - In Chrome, in the top-right corner, click the **Customize and control Google Chrome** icon. Then click **Settings**.
 - Scroll to the bottom and click Advanced.
 - Under System, click **Open proxy settings**.
- 3. Click the **Content** tab.



4. Click Certificates and then click the Trusted Root Certification Authorities tab.

Certificates ×					
Intended purpose: <all></all>	,			~	
Intermediate Certification Au	uthorities Trusted Root Co	ertification Auth	orities Trusted Publ	• •	
Issued To	Issued By	Expiratio	Friendly Name	^	
Certum CA	Certum CA	6/11/2027	Certum		
Certum Trusted Ne	Certum Trusted Netw	12/31/2029	Certum Trusted		
Class 2 Primary CA	Class 2 Primary CA	7/6/2019	CertPlus Class 2		
Class 3 Public Prima	Class 3 Public Primary	8/1/2028	VeriSign Class 3		
COMODO RSA Cert	COMODO RSA Certific	1/18/2038	COMODO SECU		
Copyright (c) 1997	Copyright (c) 1997 Mi	12/30/1999	Microsoft Timest		
DigiCert Assured ID	DigiCert Assured ID R	11/9/2031	DigiCert		
DigiCert Global Roo	DigiCert Global Root CA	11/9/2031	DigiCert		
DigiCert Global Roo	DigiCert Global Root G2	1/15/2038	DigiCert Global R	¥	
Import Export	Remove		Advan	nced	
Certificate intended purpose	25				
Server Authentication			View		
			Clos	se	

- 5. Click Import. The Welcome to the Certificate Import Wizard dialog box is displayed.
- 6. Click **Next**. The File to Import dialog box is displayed.

File to Import	
Specify the file you want to import.	
File name:	
C:\Temp\nokeywavecrest.crt	Browse
Note: More than one certificate can be stored in a single file in the fo	llowing formats:
Personal Information Exchange- PKCS #12 (.PFX,.P12)	
Cryptographic Message Syntax Standard-PKCS #7 Certificates (.F	P 7 B)
Microsoft Serialized Certificate Store (.SST)	

- 7. Click Browse to locate the downloaded certificate file. An Open dialog box is displayed.
- 8. Locate and select the certificate file.
- 9. Click **Open**. The File to Import dialog box displays the **File name** field populated with the path of the certificate file.
- 10. Click **Next**. The Certificate Store dialog box is displayed.

Certificate Store			
Certificate stores are system areas where certificates are kept.			
Windows can automatically select a certificate store, or you can specify the certificate.	a location for		
○ Automatically select the certificate store based on the type of certificate			
Place all certificates in the following store			
Certificate store:			
Trusted Root Certification Authorities	Browse		

- 11. Select the **Place all certificates in the following store** option, and click **Browse** to select *Trusted Root Certification Authorities*. Click **OK**.
- 12. Click Next. The Completing the Certificate Import Wizard dialog box is displayed.

Completing the Certificate Import Wizard					
The certificate will be imported after	The certificate will be imported after you click Finish.				
You have specified the following set	tings:				
Certificate Store Selected by User	Trusted Root Certification Authorities				
Content	Certificate				
File Name	C:\Temp\nokeywavecrest.crt				

- 13. Click Finish. A Security Warning dialog box is displayed.
- 14. Click **Yes** to install the certificate. A dialog box is displayed indicating that the import was successful.
- 15. Click **OK**. The Wavecrest Computing certificate is listed in the Trusted Root Certification Authorities tab.
- 16. Click **Close** to close the Certificates dialog box.
- 17. Click OK to close the Internet Options dialog box.

Installing the Wavecrest Certificate Using Mozilla Firefox 58

- 1. From the Firefox menu, click Options.
- 2. Click Privacy & Security and then scroll down to the Certificates section.
- 3. Click View Certificates. The Certificate Manager dialog box is displayed.
- 4. Click the **Authorities** tab.

				Certificate	Manager		>
Your Certi	ficates P	eople	Servers	Authorities	Others		
You have cer	tificates on file	e that ider	ntify these ce	ertificate authori	ties		
Certificate N	lame					Security Device	E\$
✓AC Camerfirm	a S.A.						^
Chambers o	f Commerce Roo	t - 2008				Builtin Object Token	
Global Chan	nbersign Root - 2	800				Builtin Object Token	
✓AC Camerfirm	a SA CIF A827432	87					
Camerfirma	Chambers of Co	mmerce Roo	t			Builtin Object Token	
Camerfirma	Global Chamber	sign Root				Builtin Object Token	
~ACCV							
ACCVRAIZ1						Builtin Object Token	
✓Actalis S.p.A./0	3358520967						
Actalis Auth	entication Root (Δ				Builtin Object Token	۲
<u>V</u> iew	<u>E</u> dit Trust	I <u>m</u> port	t E <u>x</u> por	t Delete or	Distrust		
							OK

- 5. On the Authorities tab, click Import.
- 6. Locate and select the certificate file.
- 7. Click **Open**. The Downloading Certificate dialog box is displayed.

Downloading Certificate	\times
You have been asked to trust a new Certificate Authority (CA).	
Do you want to trust "Wavecrest Computing, Inc. Primary EV Certificate Authority" for the following purposes?	
Trust this CA to identify websites.	
Trust this CA to identify email users.	
Trust this CA to identify software developers.	
Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).	
View Examine CA certificate	
OK Cancel	

- 8. Select Trust this CA to identify websites and click OK.
- 9. Click **OK** to close the Certificate Manager dialog box.
- 10. Close the Options tab in Firefox.

Importing the Wavecrest Certificate Using Active Directory

1. On the Active Directory server, from the Start menu, select Administrative Tools and then Group Policy Management.

Scoup Policy Management		_ 🗆 ×
ිදී Eile Action View Window Help		_ B ×
Image: Stress of the stres	Domains Contents Domain ▲ ∰Wavecave.lan	Current Domain Controller Gaels:Wavecave.lan

2. Double-click the Domains folder, your domain name, and the Group Policy Objects folder.

Sroup Policy Management				
ිදී Eile Action View Window Help				
Image: Second	CertPushTest Scope Details Settings Delege Links Display links in this location: The following sites, domains, and O Location A Support Wavecave.lan	ation Wavecave.lan !Us are linked to this GPO: Enforced No No	Link Enabled No Yes	Path Wavecave.lan/W Wavecave.lan
	Security Filtering The settings in this GPO can only a Name A Authenticated Users	pply to the following groups, u	sers, and comp	uters:

3. Right-click your Group Policy object (e.g., CertPushTest) and select Edit. The Group Policy Object Editor is displayed.



- 4. Under your Group Policy object, double-click **Computer Configuration**, **Windows Settings**, **Security Settings**, and then **Public Key Policies**.
- 5. Right-click **Trusted Root Certification Authorities**, select All Tasks and then Import. The Welcome to the Certificate Import Wizard dialog box is displayed.
- 6. Click **Next**. The File to Import dialog box is displayed.

File to Import	
Specify the file you want to import.	
File name:	
C:\Temp\nokeywavecrest.crt	Browse
Note: More than one certificate can be stored in a single file in the fo	llowing formats:
Personal Information Exchange - PKCS #12 (.PFX,.P12)	
Cryptographic Message Syntax Standard-PKCS #7 Certificates (.F	P 7 B)
Microsoft Serialized Certificate Store (.SST)	

- 7. Click Browse to locate the downloaded certificate file. An Open dialog box is displayed.
- 8. Locate and select the certificate file.
- 9. Click **Open**. The File to Import dialog box displays the **File name** field populated with the path of the certificate file.
- 10. Click **Next**. The Certificate Store dialog box is displayed.

Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
○ Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Trusted Root Certification Authorities Browse

- 11. The **Place all certificates in the following store** option is selected by default, and the **Certificate store** field is populated with "Trusted Root Certification Authorities."
- 12. Click Next. The Completing the Certificate Import Wizard dialog box is displayed.

Completing the Certificate Import Wizard					
The certificate will be imported after you click Finish.					
You have specified the following set	tings:				
Certificate Store Selected by User	Trusted Root Certification Authorities				
Content	Certificate				
File Name	C:\Temp\nokeywavecrest.crt				

- 13. Click Finish. A dialog box is displayed indicating that the import was successful.
- 14. Click **OK**. The Wavecrest Computing certificate is listed in the Group Policy Object Editor.

Installing the Wavecrest Certificate in Windows 7 Professional/Enterprise

1. From the Start menu, type *mmc* in the search box, and press **Enter**. The Console window is displayed.

Console1 - [Console Root]	vorites Window Help		
Console Root	Name	There are no items to show in this view.	Action Conse M

2. From the File menu, select Add/Remove Snap-in. The Add or Remove Snap-ins dialog box is displayed.

					Edit Extensions
ap-in	Vendor	â		Console Rooc	Euli Extensions
Active Directory Do	Microsoft Cor	=			Remove
Active Directory Site	Microsoft Cor	-			
Active Directory Use	Microsoft Cor			2	
ActiveX Control	Microsoft Cor				Move Up
ADSI Edit	Microsoft Cor				Move Down
Authorization Manager	Microsoft Cor		Add >		
Certificate Templates	Microsoft Cor				
Certificates	Microsoft Cor				
Certification Authority	Microsoft Cor				
Component Services	Microsoft Cor				
Computer Managem	Microsoft Cor				
Device Manager	Microsoft Cor				
DF5 Management	Microsoft Cor	+			Advanced
cription:					

3. Under **Available snap-ins**, select **Certificates** and click **Add**. The Certificates snap-in dialog box is displayed.

Certificates snap-in	8
This snap-in will always manage certificates for:	
My user account	
Service account	
Computer account	
< Back Finish Cance	:

4. Select **My user account** and click **Finish**. **Certificates - Current User** is displayed under **Selected snap-ins** in the Add or Remove Snap-ins dialog box.

NOTE: You may select the **Computer account** option to manage the certificate for the computer account for all users.

ActiveX Control ActiveX Control Authorization Manager Certificates Component Services Computer Manager Device Manager Disk Management Event Viewer Folder Folder Folder IP Security Monitor IP Security Monitor IP Security Policy M IP Security Policy M	Vendor Microsoft Cor Microsoft Cor	* III	Add >	Selected shap-ins:	User Edit Extensions Remove Move Up Move Down Advanced
escription: The Certificates snap-in allo	ows you to browse	the	contents of the	certificate stores for yourself,	a service, or a computer.

5. Click OK. Certificates - Current User is displayed in the Console Root folder.

Image: Second					
Console Root	Issued To	Issued By	Expirati 🔺	Actions	
Certificates - Current User	🛱 AddTrust External CA Root	AddTrust External CA Root	5/30/20	Certificates 🔺	
Personal Trusted Root Certification Authorities	🛱 Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/20	More 🕨	
Certificates	Certum CA	Certum CA	6/11/20		
Enterprise Trust	Class 3 Public Primary Certificat	Class 3 Public Primary Certificatio	8/1/202		
Intermediate Certification Authorities	Class 3 Public Primary Certificat	Class 3 Public Primary Certificatio	1/7/200		

- 6. Double-click Certificates Current User and then Trusted Root Certification Authorities.
- 7. Right-click **Certificates**, and select All Tasks and then Import. The Welcome to the Certificate Import Wizard dialog box is displayed.
- 8. Click **Next**. The File to Import dialog box is displayed.

Wavecrest Certificate SHA-512 Installation Guide

File to Import	
Specify the file you wa	nt to import.
File name:	
	Browse
Note: More than one o	ertificate can be stored in a single file in the following formats:
Personal Informatio	n Exchange- PKCS #12 (.PFX,.P12)
Cryptographic Mess	age Syntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized	Certificate Store (.SST)
Learn more about certificate	file formats
	< Back Next > Cancel

- 9. Click **Browse** to locate the downloaded certificate file. An Open dialog box is displayed.
- 10. Locate and select the certificate file.
- 11. Click **Open**. The File to Import dialog box displays the **File name** field populated with the path of the certificate file.
- 12. Click **Next**. The Certificate Store dialog box is displayed.

tificate Import Wizard		
Certificate Store		
Certificate stores are system areas v	where certificates are kept.	
Windows can automatically select a c the certificate.	certificate store, or you car	specify a location for
O Automatically select the certification	icate store based on the ty	pe of certificate
Place all certificates in the following the second seco	owing store	
Certificate store:		
Trusted Root Certification A	uthorities	Browse
earn more about <u>certificate stores</u> .		

13. The **Place all certificates in the following store** option is selected by default, and the **Certificate store** field is populated with "Trusted Root Certification Authorities."

14. Click Next. The Completing the Certificate Import Wizard dialog box is displayed.

Certificate Import Wizard		— ×		
	Completing the Certificate Import Wizard The certificate will be imported after you click Finish.			
	Contificante Chara Coloritad hu Una	Trusted Deat Cartifier		
	Certificate Store Selected by User	Trusted Root Certifica		
	Content	PFX V//development/Wev		
	The radine	r wevelopment (waw		
	•	•		
	< Back F	Finish Cancel		

- 15. Click **Finish**. A Security Warning dialog box is displayed.
- 16. Click **Yes** to install the certificate. A dialog box is displayed indicating that the import was successful.
- 17. Click **OK**. The Wavecrest Computing certificate is listed in the Trusted Root Certification Authorities, Certificates folder.

SSL Inspection

Now that you have installed the Wavecrest Certificate, you may proceed to use the SSL Inspection screen in the product.

NOTE: By enabling SSL Inspection, applications using HTTPS communication and not utilizing Windows Certificate Stores for certificate validation may encounter errors. Contact Technical Support for assistance at (321) 953-5351, Ext. 4 or support@wavecrest.net.



Wavecrest Computing

904 East New Haven Avenue Melbourne, FL 32901 toll-free: 877-442-9346 voice: 321-953-5351 fax: 321-953-5350

All specifications subject to change without notice. © Copyright 2018 Wavecrest Computing Incorporated. All rights reserved.

www.wavecrest.net