Installing and Configuring a Server Certificate for use by MailSite Fusion with TLS/SSL

A guide for MailSite Administrators

MailSite, Inc. technical White Paper

June 2008

mailsite® FUSION

Table of Contents

Introduction

MailSite 6.1 and higher provides secure messaging through the use of Transport Layer Security (TLS) and Secure Socket Layer (SSL) technology. These industry standard technologies allow for secure, encrypted email sending and retrieval between email clients and servers using certificates and public key cryptography.

MailSite requires that an appropriate certificate be installed in the Windows Certificate Store in order to enable secure communications just as a certificate is required to enable secure communication with a web server.

This white paper details MailSite, Inc's recommended procedures for the creation, installation and management of a server certificate. Refer to the MailSite Admin Guide for additional information on configuring secure messaging in MailSite Fusion.

Familiarity with Microsoft's IIS and Windows domain administration is assumed, along with a technical understanding of the Microsoft Windows operating system.

1. Creating the Initial Certificate for the Default Domain

There are four ways to obtain a certificate to enable secure communication with MailSite Fusion.

- Use an existing certificate.
- Purchase a certificate from a trusted certificate authority
- Request a certificate from a certificate authority in your domain using the Certificate Admin Website in Windows 2000
- Generate a self-signed certificate

It is recommended that you use/purchase a certificate from a trusted certificate authority such as GoDaddy, Verisign, etc. If you use a self signed certificate then your clients will get security prompts in their client telling them the certificate authority isn't trusted. A certificate from a trusted authority will prevent this. A self signed certificate is useful to test the TLS/SSL functionality and situations where you are not concerned about any security warnings on the client side.

Things that you need to consider when starting the process of creating a Certificate.

The *Common Name (CN)* of the certificate must match the hostname of the Reverse DNS (PTR) record for the IP addresses that the MailSite services are listening on or the Windows HOSTS file must be updated to override the PTR record returned by your DNS servers. MailSite Fusion does a reverse DNS lookup to find out the Common Name of the certificate to use before searching the certificate store for an appropriate certificate.

Example: The network adapters in your mail server are assigned the IP addresses 192.168.1.10 and 192.168.1.11 and your DNS servers report that the reverse DNS entries for 192.168.1.10 and 192.168.1.11 are both mail.yourcorp.com. MailSite Fusion will look for a certificate with a common name of mail.yourcorp.com in the certificate store.

If MailSite Fusion is unable to locate an appropriate certificate it will log the following error indicating the name of the Common Name of the certificate that it attempted to locate:

TLS/SSL: The service failed to find a suitable certificate in the predefined MY System store for the LocalMachine : No certificates were found matching the Subject 'smtp.yourcorp.com'.

The HOSTS file is located in the %SYSTEMROOT%\SYSTEM32\DRIVERS\ETC on your server can be updated to override the reverse DNS entries and point MailSite Fusion to the appropriate certificate.

Creating a Certificate with the Certificate Admin Website

The Certificate Admin Website can be used to request certificates for use within a Windows domain. This type of certificate is appropriate when using MailSite for secure messaging with a corporate environment where the user's desktops are members of the domain and implicitly trust the domain certificate authority.

To create a certificate in a domain you need to have the certificate authority installed on a domain controller including the Certificate Admin website component.

To install an enterprise root certification authority:

1. Log on as a member of both the Enterprise Admins group and the root domain's Domain Admins group.
2. If any Windows 2000 enterprise certification authorities (CAs) currently exist or have ever existed in your enterprise, open Certificate Templates and, when prompted to install new certificate templates, click **OK**.
3. Open Add or Remove Programs in Control Panel.
4. Click **Add/Remove Windows Components**.
5. In the Windows Components Wizard, select the **Certificate Services** check box. A dialog box appears to inform you that the computer cannot be renamed and that the computer cannot be joined to or removed from a domain after Certificate Services is installed. Click **Yes**, and then click **Next**.
6. Click **Enterprise root CA**.
7. (Optional) Select the **Use custom settings to generate the key pair and CA certificate** check box, and then click **Next** to specify the following:

To set this	Do this
Cryptographic service provider (CSP)	In **CSP**, click the CSP that you want to use. The default is the Microsoft Strong Cryptographic Provider. Certificate Services does support third party CSPs, but you must refer to the CSP vendor's documentation for information about using their CSP with Certificate Services.
Hash algorithm	In **Hash algorithm**, click the hash algorithm you want to use. The default is SHA-1.
Use an existing key	Select the **Use existing key** check box, click **Import**, and then, in **Open PFX File**, type the file name and password of the public and private key pair. This is helpful if you are relocating or restoring a previously installed certification authority (CA). Note that, when using an existing key, a new certificate is generated. **Important**: Be sure that you select an existing key that you know to be uncompromised and trustworthy. Using a key that may be compromised or untrusted could cause this CA and all its issued certificates to be insecure.
Key length	In **Key length**, type or select a key length. The default key length using the Microsoft Strong Cryptographic Provider is 2048 bits. Default key lengths for other CSPs vary. In general, the longer the key length, the more secure the key is. Also, longer key lengths require more system resources for operations such as signing, encryption, and chain verification. For a root CA, you should use a key length of at least 2048 bits. This option is not available if you use existing keys.
Allow this CSP to interact with the desktop	Select the **Allow this CSP to interact with the desktop** check box. Without this option, system services cannot interact with the desktop of the user who is currently logged on.

Import	Click **Import**. This imports an existing key in the PKCS #12 PFX format.
View certificate	Click **View certificate**. This allows you to view the certificate that you select or generate during installation.

8. When you are done, click **Next**.
9. In **Common name for this CA**, type the common name of the certification authority.
10. In **Validity period**, specify the validity duration for the root CA and click **Next**.
11. Specify the storage locations of the certificate database, the certificate database log, and the shared folder and click **Next**.
12. If Internet Information Services (IIS) is running, you will see a request to stop the service before proceeding with the installation and click **OK**.
13. If prompted, type the path to the Certificate Services installation files.

Notes:

- The preliminary information that is supplied during setup, such as the name of the certification authority, cannot be changed after the CA setup is complete.
- Before installing a certification authority, you should configure the computer's domain settings first, such as joining a domain or promoting a server to domain controller. These settings cannot be changed once the certification authority is installed.
- If Active Server Pages are not enabled through Internet Information Services, you will be prompted to activate them. The Web interface for the certification authority requires running Active Server Pages.
- The enterprise root CA selection requires that the host computer be a member of a domain and that it use the 'Active Directory' directory service. The administrator who is installing an enterprise CA must have Write permission to Active Directory.
- If you have Write permission to Active Directory, then specifying the shared folder is optional, and is not typically done for enterprise certification authorities.
- The validity duration you choose for the CA will determine when the CA "expires." For information about renewing CAs, see Related Topics.
- If you installed the enterprise certification authority as an Enterprise Admin or delegated user, then you must use the Enterprise Admin or delegated user account when you uninstall the enterprise certification authority.
- To open Add/Remove Windows Components, click **Start**, click **Control Panel**, double-click **Add or Remove Programs**, and then click **Add/Remove Windows Components**.
- Once the certification authority is installed, add certificate templates to the certification authority and configure the certification authority to allow subjects to request a certificate that is based on a template. For more information, see Related Topics.

Creating Server Certificates Using Certificate Services Web Forms

Now that you have the Domain Controller setup for issuing Certificates to your MailSite platform you need to create a certificate for your Servers.

You can use the Web forms that are included with Certificate Services 2.0 to create a key pair that is signed by your CA without having to use the Web Server Certificate Wizard. This can save time if you do not already have a site configured, but know the information needed to create the certificate for the site.

To create a server certificate, perform the following steps:

> **NOTE:** You must be an administrator to complete the following steps.

1. On the computer where the Web site will reside, browse to your certificate server's Web pages (usually located at http://*servername*/certsrv, where *servername* is the name of the server hosting IIS and the certificate server).
2. Choose **Request a Certificate**, and then click **Next**.
3. Choose **Advanced Request**, and then click **Next**.
4. Choose **Submit a Certificate Request to This CA Using a Form**, and then click **Next**.
5. From the **Certificate Template Select** '**Web Server**'**.** If this is not available please see the troubleshooting section.
6. Under **Identifying Information**, in the **Name** field, choose a common name for the Web site. For example, if the default domain is "Example.com" and the DNS name is "mail.example.com", then the common name would be "mail.example.com."
7. For the rest of the information under **Identifying Information**, follow the instructions for email, company, and so on.
8. In the **Intended Purpose** section, choose **Server Authentication Certificate** from the drop-down list.
9. In the **Key Options** section, under **CSP** choose "Microsoft RSA SChannel Cryptographic Provider' with a **Key Size** of **1024 or 2048**.
10. Be sure to enable the **Mark Private Key as Exportable** check box if you want to backup this key pair later (recommended). *If you do not do this, you will not have the option to export the private key at a later time (only the public key)*.
11. Click **Submit**.
12. When you are prompted to 'Install the Certificate', do so. This adds the certificate to your certificate store (the local computer store).

Troubleshooting Issues with Certificate Admin Website

If the Certificate Admin Website only shows in the Custom Templates, User and Basic EFS follow these steps to resolve it:

1. From a domain controller, log on to the parent domain with a user account that has membership in the Enterprise Administrators group.
2. Click Start, click Programs, click Administrative Tools, and then click the "Active Directory Sites and Services" snap-in.
3. In MMC, right-click the "Active Directory Sites and Services" snap-in, click View, and then click "Show Services Mode". This allows you to view the Services folder, which is hidden from view by default.
4. From the "Active Directory Sites and Services" snap-in, click Services, click Public Key Services, and then click Certificate Templates. This reveals the complete list of published certificate templates in Active Directory.
5. Double-click the User certificate template to view the properties.
6. On the Security tab, click Add to add the Domain Users group of the child domain to the list.
7. For the Domain Users (<CHILDDOMAINNAME>\Domain Users) group, select the Read and Enroll rights.
8. Restart the computer.

Generating a Certificate Request File Using the Certificate Wizard in IIS 6.0

As we have stated there are two ways to generate a Certificate and this is the second way to create a certificate. Follow these steps if you wish to obtain a 3rd party Certificate.

The Certificate Wizard that comes with Internet Information Services (IIS) 6.0 makes managing server certificates easier than ever before. This section describes how to create a ***certificate request file*** using the wizard.

The first step to get a server certificate is creating the request file. To generate a new certificate request (to be sent to a ***certificate authority*** or CA for processing), perform the following steps:

> **NOTE**: The certificate request fails if it contains non-alphanumeric characters. **NOTE**: Between creating the request file (that is, completing the steps in this section) and installing the certificate, do **NOT** perform any of the following actions:
>
> - Change the computer name or Web site bindings.
> - Apply service packs or security patches.
> - Change encryption levels (that is, apply the high encryption pack).
> - Delete the pending certificate request.
> - Change any of the Web site's Secure Communications properties.

1. Open the Internet Services Manager (or your custom MMC containing the IIS snap-in).

2. Browse to the site where you want to enable secure communications.
3. Right-click the friendly name of the site and go to properties.
4. Click the **Directory Security** tab.
5. Under the Secure Communications section, click **Server Certificate**.
6. This starts the new Web Site Certificate Wizard.
7. Click **Next**.
8. Choose the Create a New Certificate option and click Next (there should be a slight pause before the next screen appears).
9. Choose the **Prepare a New Request but Send it Later** option, click **Next**.

   > **NOTE**: The **Send the request immediately to an online certification authority** option is unavailable unless IIS has access to an Enterprise CA, which requires Certificate Server 2.0 to be installed in Microsoft Windows 2000 with Active Directory.

10. Choose a Friendly Name for the site (this can be anything you want it to be, for example, the friendly name of the site in the MMC, or the name of the customer the Web site belongs to).
11. Choose the bit length of the key you want to use which for MailSite Fusion is 1024 or 2048 and select 'Select cryptography service provider (CSP) for this certificate', and then click **Next**.
12. For the 'Available Providers' highlight 'Microsoft RSA SChannel Cryptographic Provider'. Then click **Next**.
13. Input your Organization (O) and your Organizational Unit (OU). For example, if your company is called Widgets and you are setting up a Web server for the Sales department, you would enter Widgets for the Organization and Sales for your Organizational Unit. Click **Next** when complete.
14. Input the common name (CN) for your site. This should be the same name that the Mail Servers will connect with to send mail. For example, if a mail server connects to mail.example.com to send mail to the Mail Server, then your Common Name would be mail.example.com. When you are complete, click **Next**.
15. Input your Country/Region, City, and State. It is very important that you do not abbreviate the names of the state or city. When complete, click **Next**.
16. Choose a name for the certificate request file you are about to create. This file will contain all the information you created here, as well as your public key for your site. You can browse the file name if you want. This creates a .txt file when you are complete. The default name for the file is Certreq.txt. When you have finished this step, click **Next**.
17. You will now be presented with a summary screen of all the information you entered. Make sure all this information is correct, and then click **Next**.
18. You have now created your certificate request file.

In order for this certificate to be used, submit this file to a Certificate Authority (online authority). They will generate a certificate response file, which contains your public key and is digitally signed by the Certificate Authority.

2. Installing a New Certificate with Certificate Wizard for Use in SSL/TLS

In order to provide secure communications (SSL/TLS) to your MailSite server, a server certificate is required on the server that you want to provide the email service from.

Before the following steps can be completed, you must first generate a certificate request, and then send it to an online authority (certificate authority). If you have not done this, perform the steps is section '***Generating a Certificate Request File Using the Certificate Wizard in IIS 6.0'.*** When you receive your response file from the online authority, you will need to install this on the Mail server.

> **NOTE**: The response file contains your public key that has been signed by the authority. A client can successfully connect to the site without trusting the authority who issued the server certificate. However, if the client does not trust the authority, it is likely to warn the end-user each time it connects. Typically the client will issue a security prompt that says something such as "The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority." The end-user is given the option to continue or view the certificate at this point.

To install the response file, follow these steps:

1. Click **Start**, and then click **Run**.
2. Type in "MMC.EXE" (without the quotation marks) and click **OK**.
3. Click **Console** in the new MMC you created, and then click **Add/Remove Snap-in**.
4. In the new window that appears, click **Add**.
5. Highlight **Certificates,** and then click **Add**.
6. Choose the **Computer account** option and click **Next**
7. Select **Local Computer** on the next screen, and then click **OK**.
8. Click **Close**, and then click **OK**.

You have now added the Certificates snap-in, which will allow you to work with any certificates in your computer's certificate store. You may want to save this MMC for later use.

1. Open the Certificates (Local Computer) snap-in you added in the last section, navigate to **Personal**, and then to **Certificates**.
2. Right-click **Certificates** (or **Personal** if that option does not exist.)
3. Choose **All Tasks**, and then click **Import**.
4. When the wizard starts, click **Next**. Browse to the file sent to you by the Certificate Authority.
5. Click **Next**, and then choose the Certificate Store you want to save the certificate to. You should select **Personal** because it is a Web server certificate. If you included the certificates in the certification hierarchy, it will also be added to this store.

6. Click **Next**. You should see a summary of screen showing what the wizard is about to do. If this information is correct, click **Finish**.
7. You will now see the server certificate for your server in the list of Personal Certificates. It will be denoted by the common name of the server (found in the subject section of the certificate).

You now have a server certificate installed.

3. Backing Up a Server Certificate

You may want to back up your server certificate(s). Windows 2000 makes this process easy using the new Certificates snap-in.

Create an MMC Snap-in for Managing Certificates

In order to perform the backup, you must first create a new MMC and add the Certificates snap-in. You can also add the snap-in to another MMC as long as it is opened in Author mode.

Use the following steps to create a new MMC and add the Certificates snap-in:

1. Click **Start**, and then click **Run**.
2. Type in "MMC.EXE" (without the quotation marks) and click **OK**.
3. Click **Console** in the new MMC you created, and then click **Add/Remove Snap-in**.
4. In the new window that appears, click **Add**.
5. Highlight **Certificates**, and then click **Add**.
6. Choose the **Computer account** option and click **Next**
7. Select **Local Computer** on the next screen, and then click **OK**.
8. Click **Close**, and then click **OK**.

You have now added the Certificates snap-in, which will allow you to work with any certificates in your computer's certificate store. You may want to save this MMC for later use.

Export a Certificate and Public Key

Now that you have added the Certificates snap-in, you can export the key pair that your Server is using (the certificate and public key). To do this, perform the following steps:

1. Open the Certificates (Local Computer) snap-in you added in the last section, navigate to **Personal**, and then to **Certificates**.
2. You will see your Web server certificate denoted by the CN (Common Name) found in the Subject field of the certificate (using Internet Explorer, you can easily view the certificate to see the Common Name if you are unsure).
3. Right-click on the server certificate, select **All Tasks**, and then click **Export**.
4. When the wizard starts, click **Next**. Choose to export the private key, and then click **Next**. **NOTE**: If you export the certificate do not select **Require Strong Encryption**. This option causes a password prompt every time an application attempts to access the private key.
5. The file format you will want to choose is the **Personal Information Exchange** (though you can select from several options). This will create a PFX file. Notice that you can export any certificates in the certification path by selecting the option on this screen. This is very handy if your certificate was

issued by a non-trusted certificate authority (for example, Microsoft Certificate Server). Only choose delete the private key if the export is successful to be sure it is not left on the computer (for example if you are migrating from one server to another).**NOTE**: If you do not select "Include all certificates in the certificate path if possible" and the issuer of the certificate is not trusted by your server, then you may notice that when the properties of the certificate are viewed, the "This certificate is issued to:" field may display "Windows does not have enough information about this certificate". This is by design and can be resolved by selecting "Include all certificates in the certificate path" while exporting the certificate.

6. Click **Next**, and then choose a password to protect the PFX file. You will need to enter the same password twice to ensure that the password is typed correctly. When you have completed this step, click **Next**.
7. Choose the file name you want to save this as. Do not include an extension in your file name; the wizard will automatically add the PFX extension for you.
8. Click **Next**, and then read the summary. Pay special attention to where the file is being saved to. If you are sure the information is correct, choose **Finish**.

You now have a PFX file containing you server certificate and its corresponding private key. Be sure to protect this file! You may want to move it to a floppy disk and store it somewhere safe from outside disturbance. Keep in mind, if you run a backup on the server, this file may be saved in that backup if it is still on the server.

How to Import a backup Server Certificate

You may want to restore a server certificate, for example, if you are migrating from one server to another. This task is very easy to do using the Web Site Certificate Wizard and the Certificate Manager Import Wizard provided to you by Windows 2000.

In order to complete this operation, you must have a backup of the server certificate (and private key) contained in a PFX file. You must also have access to the Certificates snap-in and have it set to view computer certificates from the local computer (though this can be done remotely).

In order to view the Certificates store on the local computer, perform the following steps:

1. Click **Start**, and then click **Run**.
2. Type "MMC.EXE" (without the quotation marks) and click **OK**.
3. Click **Console** in the new MMC you created, and then click **Add/Remove Snap-in**.
4. In the new window, click **Add**.
5. Highlight the **Certificates** snap-in, and then click **Add**.
6. Choose the **Computer** option and click **Next**.
7. Select **Local Computer** on the next screen, and then click **OK**.
8. Click **Close,** and then click **OK**.

9. You have now added the Certificates snap-in, which will allow you to work with any certificates in your computer's certificate store. You may want to save this MMC for later use.

Now that you have access to the Certificates snap-in, you can import the server certificate into you computer's certificate store by following these steps:

1. Open the Certificates (Local Computer) snap-in and navigate to **Personal**, and then **Certificates**.
   Note: Certificates may not be listed. If not, there are no certificates installed.
2. Right-click **Certificates** (or **Personal** if that option does not exist.)
3. Choose **All Tasks**, and then click **Import**.
4. When the wizard starts, click **Next**. Browse to the PFX file you created containing your server certificate and private key. Click **Next**.
5. Enter the password you gave the PFX file when you created it. Be sure the **Mark the key as exportable** option is selected if you want to be able to export the key pair again from this computer. As an added security measure, you may want to leave this option unchecked to ensure that no one can make a backup of your private key.
6. Click **Next**, and then choose the Certificate Store you want to save the certificate to. You should select **Personal** because it is a Web server certificate. If you included the certificates in the certification hierarchy, it will also be added to this store.
7. Click **Next**. You should see a summary of screen showing what the wizard is about to do. If this information is correct, click **Finish**.
8. You will now see the server certificate for your server in the list of Personal Certificates. It will be denoted by the common name of the server (found in the subject section of the certificate).

4. Configuring Certificate Permissions

Winhttpcertcfg.exe: WinHTTP Certificate Configuration Tool

This section details the use of this tool when you have the MailSite services in secure mode, i.e. not running under the 'LocalSystem' account. It gives background as to what the utility does and what each command means.

WinHTTP Certificate Configuration Tool (WinHTTPCertCfg) is a command-line tool that enables administrators to import certificates and their private keys for use on client computers.

Corresponding Operating System Features

Users can export and import client certificates by using a Web browser such as Internet Explorer. However, importing a certificate only allows access to that certificate's private key for the original account which installed the certificate. To grant access to other user accounts, you need WinHTTPCertCfg.

Examples

Concepts
Windows Hypertext Transfer Protocol (HTTP) Services (WinHTTP) implements the client side of the HTTP protocol on a server running Windows Server 2003. WinHTTP replaces WinInet as an HTTP client application programming interface (API) platform because of its ability to support middle-tier and server applications.

System Requirements
The following are the system requirements for this tool:

1. Windows 2000 with Service Pack 3, Windows XP Professional with Service Pack 1, or Windows Server 2003 operating system.
2. Membership in the Administrators local or domain local group.
3. If the client certificate is installed before WinHTTPCertCfg is used, the user of the tool must be the same user account that installed the certificate.

File Required: Winhttpcertcfg.exe

Syntax & Parameters

WinHTTPCertCfg uses the following syntax:

winhttpcertcfg [{**/i** *PFXFile*|**/g**|**/r**|**/l**}] **/c** {**LOCAL_MACHINE**|**CURRENT_USER**} *CertStore* [**/a** *Account*] [**/s** {*SubjectStr*] [**/p** *PFXPassword*]

/i *PFXFile*	Imports a certificate and its private key from a PFX file. When this parameter is used, the **/a** and **/c** parameters are also required.
/g	Allows the specified user account access to a certificate's private key. When this parameter is used, the **/a**, **/c**, and **/s** parameters are also required.
/r	Denies the specified user account access to a certificate's private key. When this parameter is used, the **/a**, **/c**, and **/s** parameters are also required.
/l	Lists user accounts that have access to the private key of the specified certificate. When this parameter is used, the **/c** and **/s** parameters are also required.
/c {**LOCAL_MACHINE**|**CURRENT_USER**} *CertStore*	Specifies the location and the name of the certificate store. Choose from the **LOCAL_MACHINE** or the **CURRENT_USER** hive of the registry. Select **LOCAL_MACHINE** for all users of the local computer to use the certificate. Select **CURRENT_USER** for only a particular user on the local computer to use the certificate. *CertStore* specifies the name of the certificate store that contains the certificate you need to find.
/a *Account*	Specifies a user account. This can be a local or a domain user account.
/s {*SubjectStr*	Specifies a string of characters, which WinHTTPCertCfg uses to find a certificate. WinHTTPCertCfg searches the Subject field of certificates that are present on the local computer. This string is not case-sensitive.
/p {*PFXPassword*	Specifies a password to use when importing a certificate and its private key. This parameter is only available when you use the **/i** parameter.

Example 1: List Accounts with Access to a Certificate's Private Key

The task in this example is to list the user accounts that have access to the private key of a specified certificate. To do this, use the **/l** parameter, which requires the **/c** and **/s** parameters. The certificate store, named Root, is located in the LOCAL_MACHINE hive of the registry. The name of the certificate is Test. Type the following at the command line:

winhttpcertcfg /l /c local_machine\root /s test

Press ENTER. Output similar to the following is displayed:

```
Microsoft (R) WinHTTP Certificate Configuration Tool
Copyright (C) Microsoft Corporation 2001.

Matching certificate:
CN=test
DC=contoso
DC=com
```

Additional accounts and groups with access to the private key include:
BUILTIN\Administrators
NT AUTHORITY\SYSTEM

Example 2: Grant Access to a Private Key from a User Account

The task in this example is to grant access to a certificate's private key to a user account. To do this, use the **/g** parameter, which requires the **/c**, **/s**, and **/a** parameters. The certificate store, named Root, is located in the LOCAL_MACHINE hive of the registry. The name of the certificate is Test and the user account that access is being granted to is named Testuser. Type the following at the command line:

winhttpcertcfg /g /c local_machine\root /s test /a testuser
Press ENTER. Output similar to the following is displayed:

```
Microsoft® WinHTTP Certificate Configuration Tool
Copyright© Microsoft Corporation 2001.

Matching certificate:
CN=test
DC=contoso
DC=com

Granting private key access for account:
    CONTOSO\testuser
```

References

The material in this document is compiled from numerous sources; in particular the Microsoft Windows® help files. It is therefore recommended that the latest help files for your specific operating system are consulted for the most accurate information.

Additional information can be found in the operating system help files or on Microsoft's website.

Please see the Section on Transport Layer Security in the Security chapter of the MailSite Administration Guide.

About MailSite Software Incorporated

MailSite Software Incorporated develops a low cost alternative to Microsoft Exchange for carriers, telcos, service providers, enterprises and businesses worldwide. MailSite Inc was established in 1995 under the name Rockliffe and is based in California's Silicon Valley with European headquarters in the UK. MailSite, Inc has more than 2,000 customers hosting more than 15 million mailboxes worldwide. These include service providers such as Verizon, eChalk, NetOne and WestNet, and enterprises such as Teleflora, Encyclopædia Britannica, and MediaNews Group. MailSite partners include HP, Qualcomm, J2, Cegedim Rx, Rockwell Collins, Kaspersky and Mailshell.

Disclaimer

Although MailSite Software Incorporated has made reasonable efforts to ensure the accuracy at the time of publication, the accuracy of the information contained in this guide is not guaranteed. It is provided free of charge by MailSite, Inc. and has been prepared and validated on MailSite, Inc. test and production platforms. MailSite, Inc. disclaims all warranties, either express or implied, regarding this document and MailSite, Inc. is not liable for any damages arising directly or indirectly from the information in this document.

MailSite Professional Services

MailSite Professional Services cover remote and onsite assistance with performance tuning, migrations, integrations, upgrades, email security audits, training, and custom software development. To discuss your requirements and arrange for a quote please contact **sales@mailsite.com**.

www.mailsite.com