Cisco MSI Deployment Guide

Cisco MSI Installation Guide for Microsoft Windows v1.0

Contents

1 Preface

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

2 Introduction

The Cisco Media Services Interface (MSI) provides a comprehensive, consistent and easy-to-use interface that enables applications on rich media endpoints to use Medianet[1] network services. The endpoints can use Cisco MSI to send valuable information about the media flows to the network, making the network media-aware and armed with important information that can be used to make intelligent decisions. The endpoints also become network aware and can request intelligent network services, for example, for troubleshooting.

This guide is for customers who are installing Cisco MSI on a Microsoft Windows or an Apple Mac OS X machine.

3 Supported Platforms

Cisco MSI is supported on both 32- and 64-bit versions of the following operating systems:

- Microsoft Windows 7
- Microsoft Windows 8
- Apple OS X v10.7 Lion
- Apple OS X v10.8 Mountain Lion

[1] http://www.cisco.com/go/medianet

4 Deploying Cisco MSI on Windows

The Cisco MSI Runtime package must be predeployed on a Windows user machine for compatible applications to use Cisco MSI services. It is distributed as a Windows installer package (.msi) or a self-contained runtime executable (.exe) and can be installed if needed without any user interaction (Section 4.2: Silent Installation).

There is only one version of this Runtime package, which is valid for both 32-bit x86 and 64-bit x64 architectures. The files are installed in the following locations:

- /Program Files/Cisco Systems/Media Services Interface (32-bit platforms)
- /Program Files (x86)/Cisco Systems/Media Services Interface (64-bit platforms)

Note that you must have administrative privileges to run the installer.

The following components are installed:

- The Cisco Media Services Interface Protocol Driver, a device driver that is signed with a VeriSign certificate and a Microsoft/VeriSign cross-signing certificate.

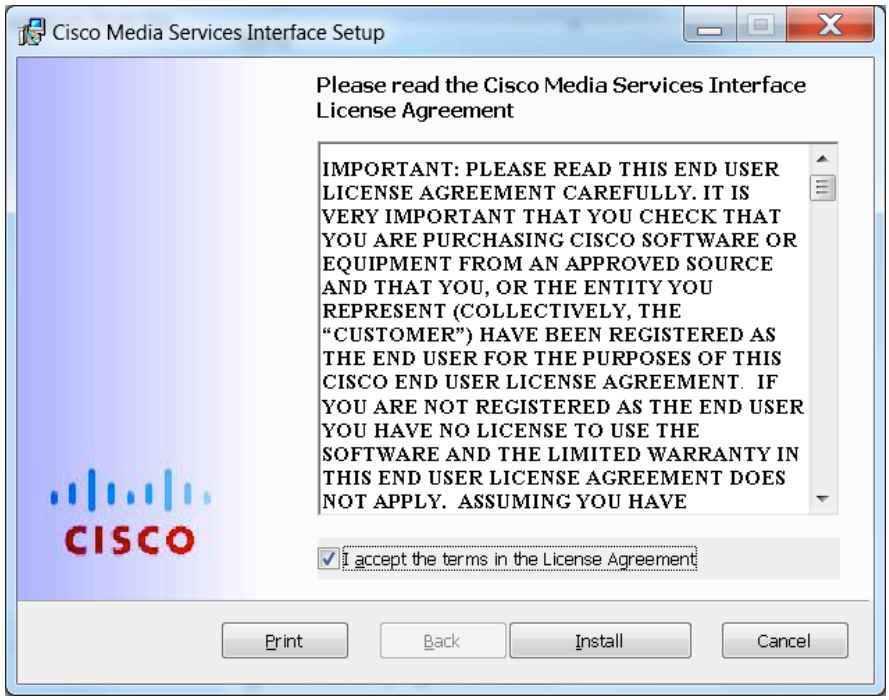
- The Cisco Media Services Interface service, a Windows service, automatically started at boot time, which runs under the "Local System" account. It is configured to log to the Windows Event Log (see Appendix B: Troubleshooting for more details about logging).

4.1 Manual Installation

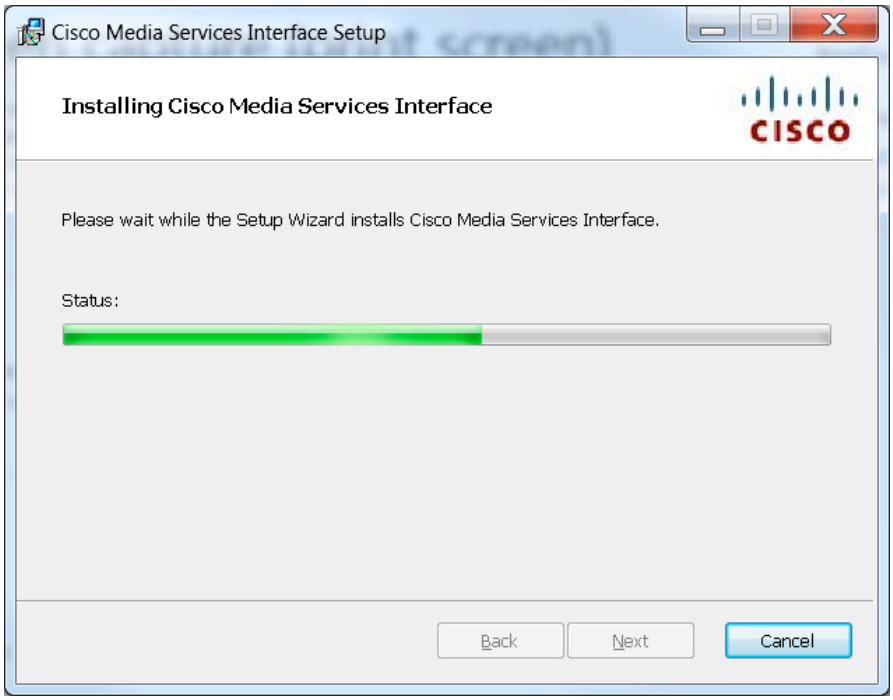
To install Cisco MSI to your Windows machine, complete the following steps:

1. Run the Installer as an administrator.

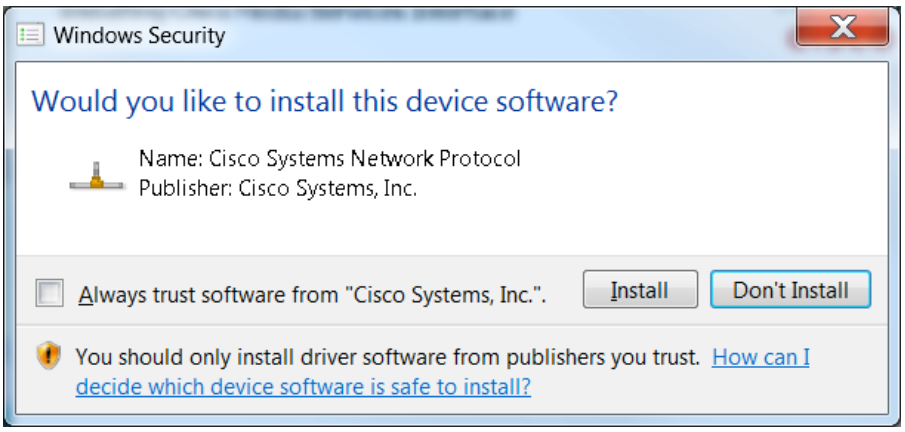
2. Read and accept the Cisco Media Services License Agreement. Click **Install** to proceed.



3. Wait until the installation is completed.

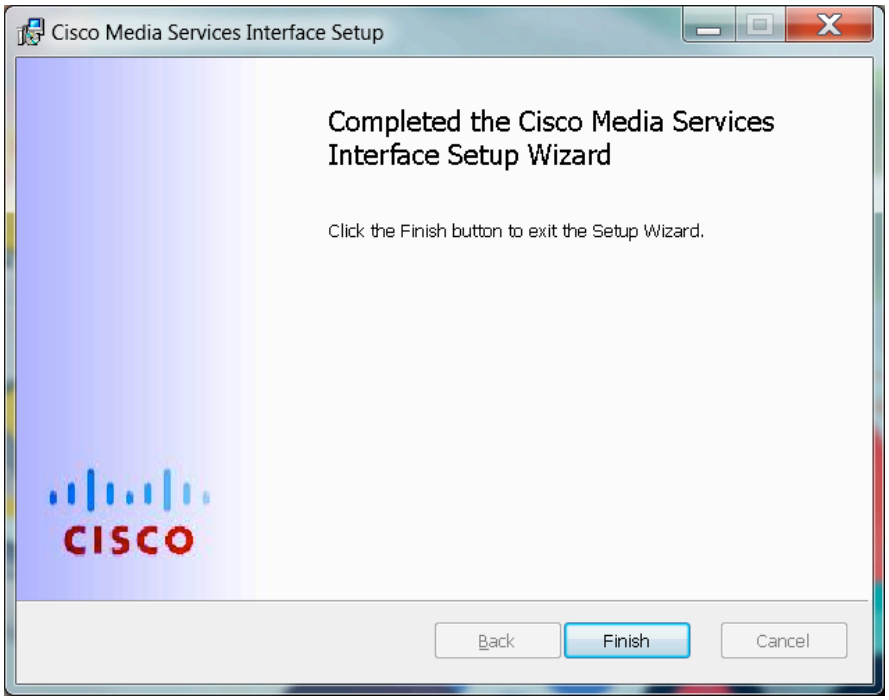


4. If the following Windows Security popup window appears, click **Install** to proceed with the installation.



This popup window asks you to confirm that you agree to install the MSI Protocol Driver. Note that this confirmation is required by Windows even though the device driver is signed with valid certificates (see Appendix A: Silent Installation on Windows for details and silent installation instructions).

5. If the following dialog box appears, you have successfully installed Cisco MSI. Click **Finish** to complete the installation.



6. If the installation fails, the following dialog box appears. See Appendix B: Troubleshooting for instructions on how to troubleshoot your problem.

4.2 Silent Installation

You can install Cisco MSI with no user interface and no user interaction. To launch a silent installation, use the Microsoft Windows Installer program **msiexec** from the command line (requires administrative privileges). Run the following **msiexec** command:

```
msiexec /quiet /i msi_setup_$version.msi
```

Note that, on Windows 7 and 8, a Windows Security popup window requires manual confirmation and therefore blocks the silent installation. For the solution to this problem, see Appendix A: Silent Installation on Windows.

4.3 Firewall Configuration

Medianet features such as Metadata or Mediatrace use the Resource Reservation Protocol (RSVP). By default, the Windows Firewall blocks all incoming traffic on non-TCP and non-UDP protocols. Therefore, for Cisco MSI to run properly, you must add a firewall rule to allow incoming RSVP traffic. The Cisco MSI service automatically adds an "allow RSVP" firewall rule at startup and removes it at shutdown.

If a third-party firewall is running in the machine, you must manually configure a firewall rule to enable RSVP incoming traffic.

4.4 Uninstalling Cisco MSI

You can uninstall the Cisco MSI (service and protocol driver) from the Add/Remove Programs area of the Control Panel. Alternatively, run the following **msiexec** command:

```
msiexec /x msi_setup_$version.msi
```

If the Cisco MSI service is running, it will be stopped, and all the client applications that are using Cisco MSI will no longer have access to its features.

4.5 MSI certificate deployment with Active Directory

The Media Services Interface (MSI) software uses X.509 certificates over TLS to provide authentication, authorization and confidentiality services for the MSIREST and MSI2MSI protocols.

MSI is able to adapt to any certificate enrollment and provisioning technique used by the platform integrator or system administrator.

This part explains how to use the Microsoft Active Directory (AD) infrastructure to deploy the certificates needed by MSI to support MSI Management via HTTP REST. Since AD is widely present in enterprise environments, its database of provisioned machine and user accounts can be successfully exploited to provide certificate deployment with zero user intervention.

Note: the text in italics is quoted from several Microsoft sources. See the References at the end of each section and the end of the document.

4.5.1 Requirements

- Active Directory Domain Services (AD DS) is installed and running as explained in [Windows Server 2008 R2 Core Network Guide].
- Active Directory Certificate Services (AD CS) is installed and running as explained in [Active Directory Certificate Services]. When creating the Root CA leave the default values as explained in section 4.5.6.2
- Web Enrollment is installed according to the instructions explained in [Setup Certification Authority Web Enrollment]. Https connection is recommended.
- *To perform auto-enrollment of client computer and enrollment of user certificates, your CA must be running the Windows Server 2008 or Windows Server 2008 R2 Enterprise operating system or the Windows Server 2008 or Windows Server 2008 R2 Datacenter operating system and must be an issuing CA* [Deploying Computer and User Certificate]

4.5.2 Technical Overview

This section provides a technical overview of AD CS, auto-enrollment, group policy and Windows certificate store.

4.5.2.1 AD CS

AD CS in Windows Server 2008 R2 provides customizable services for creating and managing X.509 certificates [...]. Organizations can use AD CS to enhance security by binding the identity of a person, device, or service to a corresponding public key. AD CS also includes features that allow you to manage certificate enrollment and revocation in a variety of scalable environments [Deploying Computer and User Certificate].

4.5.2.2 Auto-enrollment

When you deploy certificates using auto-enrollment, you configure the CA to automatically enroll certificates to computers that are members of the Domain Computers group and to users who are members of the Domain Users group. When a computer receives a computer certificate or user certificate from the CA, the certificate is stored locally in a data store named the certificate store.

You do not have to auto-enroll certificates to all members of the Domain Users and Domain Computers groups. Instead, you can issue certificates to subsets of the Domain Users and Domain Computers groups, such as to the Sales team or the Accounting department. To enroll

certificates to other groups, create the groups and then add members to the groups in Active Directory Users and Computers. In the Certificate Templates snap-in, remove the Domain Users or Domain Computers groups from the access control list (ACL) on the certificate templates (the User template and the Workstation Authentication template, respectively), and then add the groups that you created to the template [Deploying Computer and User Certificate].

4.5.2.3 Group Policy

Group Policy in Windows Server 2008 R2 is an infrastructure used to deliver and apply one or more desired configurations or policy settings to a set of targeted users and computers within an Active Directory environment. This infrastructure consists of a Group Policy engine and multiple client-side extensions (CSEs) responsible for reading policy settings on target client computers. Group Policy is used in this scenario to enroll and distribute certificates to users, computers, or both [Deploying Computer and User Certificate].

4.5.2.4 Certificate store

On computers that are running the Windows operating system, certificates that are installed on the computer are kept in a storage area called the certificate store. The certificate store is accessible using the Certificates Microsoft Management Console (MMC) snap-in.

This store contains multiple folders, where certificates of different types are stored. For example, the certificate store contains a Trusted Root Certification Authorities folder where the certificates from all trusted root CAs are kept.

When your organization deploys a PKI and installs a private trusted root CA using AD CS, the CA automatically sends its certificate to all domain member computers in the organization. The domain member client and server computers store the CA certificate in the Trusted Root Certification Authorities folder in the Current User and the Local Computer certificate stores. After this occurs, the domain member computers trust certificates that are issued by the trusted root CA.

Similarly, when you auto-enroll computer certificates to domain member client computers, the certificate is kept in the Personal certificate store for the Local Computer. When you auto-enroll certificates to users, the user certificate is kept in the Personal certificate store for the Current User [Deploying Computer and User Certificate]

4.5.2.4.1 Certificate store nomenclature

As a reminder, public-key cryptography involves two keys: a private key and a public key. Both belong to the same entity. The private key must be protected and kept secret; the public key can be made public.

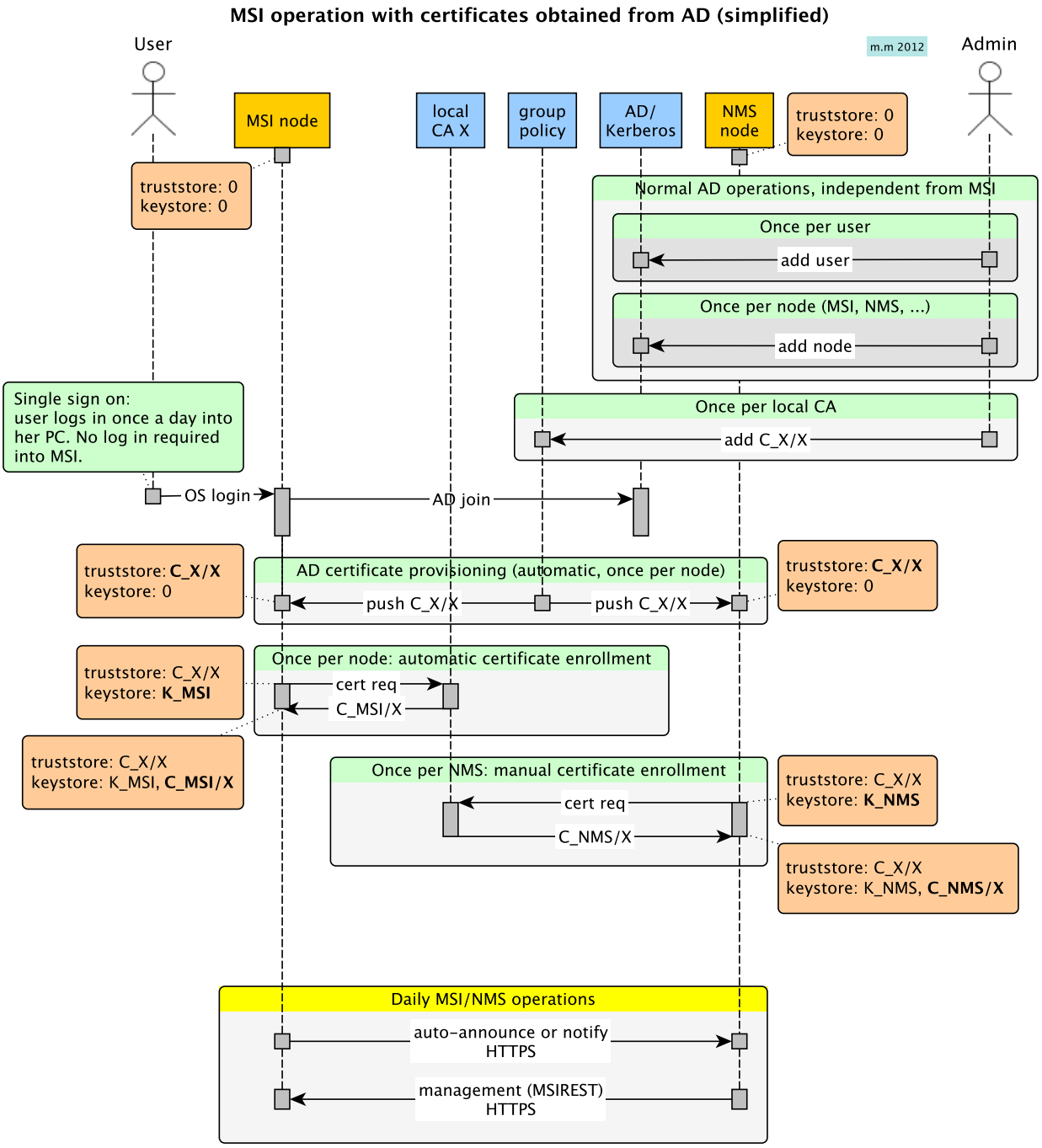
A *certificate* contains the public key of the subject, the signature of the issuer (the CA) and some metadata.

The term *certificate* is normally used in an incorrect way: sometimes it refers to a proper certificate, which is a signed public key used to trust an external entity; sometimes it refers to the pair (private key, signed public key).

To make the difference explicit, the literature uses the terms *key store* to refer to a store of (private key, signed public key) pairs, and the term *trust store* to refer to a store of signed public keys.

Microsoft Windows on the other hand uses the term *Certificate store* to refer to both usages; inside a certificate store the logical view called *Personal certificate store* refers to the key store. A Windows computer has multiple certificate stores; at least the Local computer certificate store and then a certificate store per local user.

4.5.3 Flow Overview



4.5.4 Supported Deployment Scenarios

This guide supports the following deployment scenarios:

4.5.4.1 Windows PC with Computer Account in AD domain

Requirement: The Windows PC has a Computer Account in the Active Directory, i.e. is part of the domain.

Action: The PC automatically auto-enrolls for a Computer certificate. MSI running on the PC selects the certificate used by the REST interface.

User interaction: not required.

4.5.4.2 NMS registered in AD domain

Requirement: the NMS has a User Account in Active Directory. The computer can but does not have to be part of the AD domain.

Action: The NMS user manually enrolls for a NMS User certificate. This certificate is used to interact with the REST interface in MSI.

User Interaction: required

Note: It is possible for a computer to be at the same time an NMS and an MSI end-point: no particular procedures are needed.

4.5.5 Unsupported Deployment Scenarios

This guide does not cover certificate deployment for devices that are non-Windows PCs (Mac OS X, Linux, embedded devices, etc.). This does not mean that it is not possible to use AD to deploy certificates on such devices but simply such scenarios are not covered.

Note that any design decision taken in this guide assumes that certificate deployment for such devices will be performed via Simple Certificate Enrollment Protocol (SCEP).

Additional information will be provided in following versions of this guide.

4.5.6 Certificate Deployment

4.5.6.1 Certificate Requirements

MSI uses standard X.509 certificates with the IETF PKIX profile [RFC5280] for authentication and authorization.

Authentication is performed via the normal characteristics of a certificate, by verifying the issuer and the subject identity.

Authorization is performed via a private key purpose to be added to the *Extended Key Usage* standard extension (also called *Application Policies Extension* in Windows terminology).

The OID arc 1.3.6.1.4.1.9.21.2.2 stems from the Cisco PKI OID arc and is used for Cisco MSI purposes.

4.5.6.1.1 NMS Administrator Certificate

The NMS User Certificate with Administrator role must be configured with the following purposes in Extended Key Usage (Application Policies) extension:

- Standard key purposes:
  - Client Authentication (needed by TLS)
  - Server Authentication (needed by TLS)
- Private Key purposes:
  - "Cisco Medianet MSI NMS admin" (1.3.6.1.4.1.9.21.2.2.1.1). Mandatory for an MSI to authorize the certificate owner as NMS.
  -

4.5.6.1.2 MSI Computer Certificate

The MSI Computer Certificate must be configured with the following purposes in Extended Key Usage (Application Policies) extension:

- Standard key purposes:
  - Client Authentication (needed by TLS)
  - Server Authentication (needed by TLS)
- Private Key purposes:
  - "Cisco Medianet MSI endpoint" (1.3.6.1.4.1.9.21.2.2.2). Recommended for an NMS to authenticate the certificate owner as an MSI.

4.5.6.2 Root CA Requirements

MSI REST selects the root CA certificate from the Windows certificate store based on the Subject field. The Subject field must contain the DC values equal to the Active Directory domain. Leaving the default configuration when installing the Active Directory Domain Services will set the right values. See the following picture for an example: the default values are left unchanged.

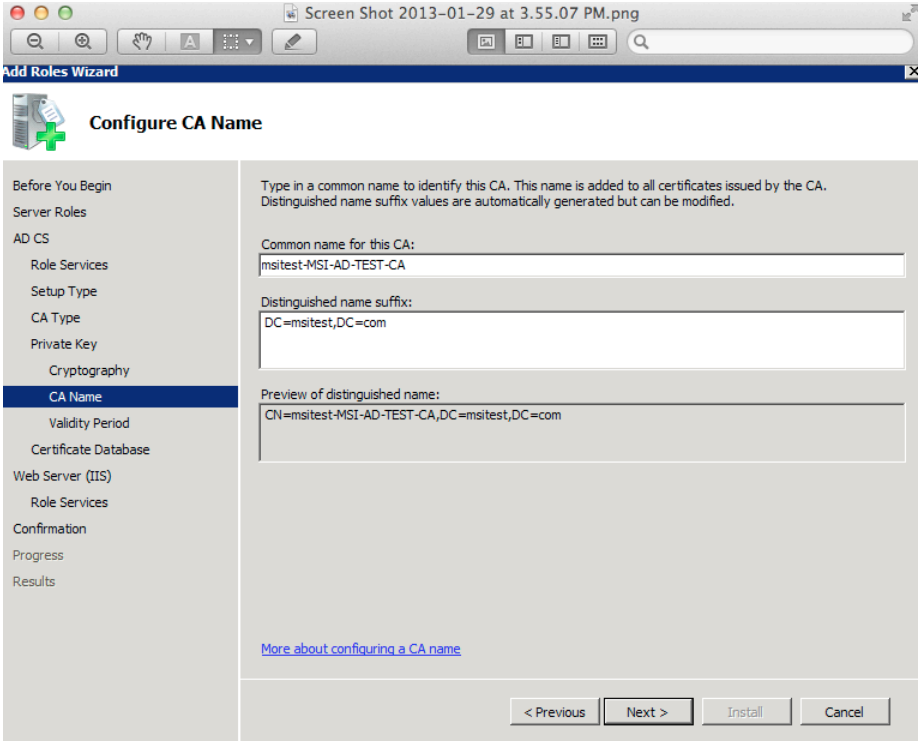
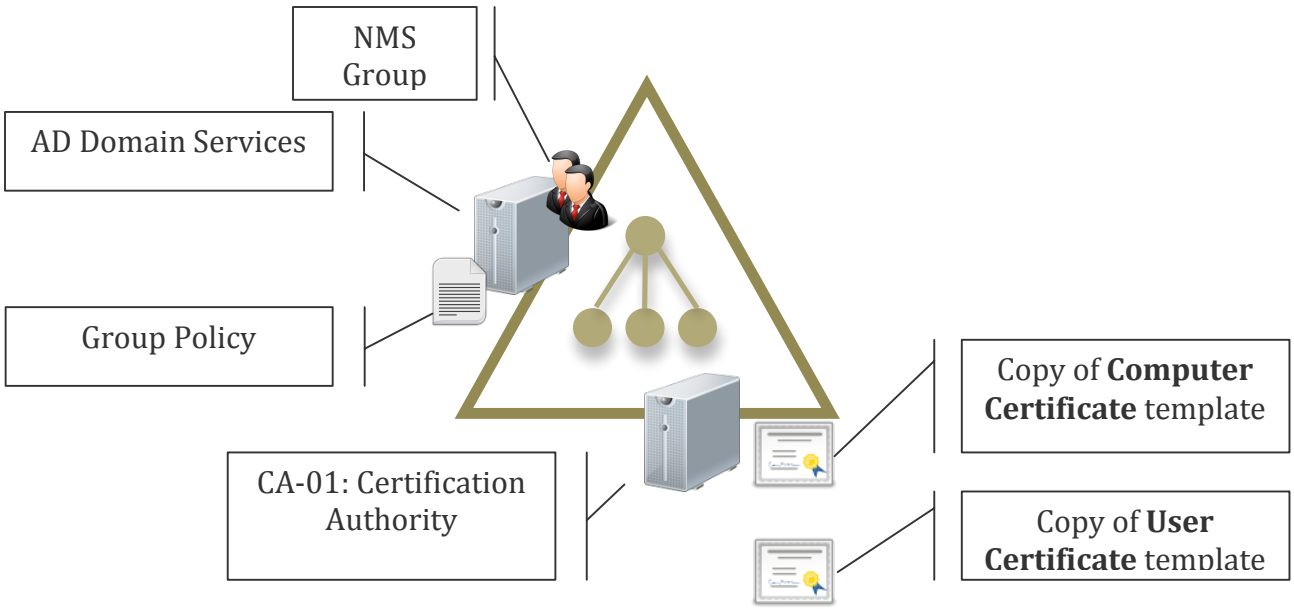


Figure 1: Default values for configuring Root CA

4.5.6.3 Deployment Components

The following figure shows the different components needed to deploy computer certificate for the MSI and user certificate for the NMS:



- **AD CS.** *The enterprise root certification authority (CA) is also an issuing CA. The CA issues certificates to computers and users that have the correct security permissions to enroll a certificate. Active Directory Certificate Services (AD CS) is installed on CA-01* [Deploying Computer and User Certificate].
- **Group for NMS.** A special group for the Network Management Stations (NMS) with administrator role needs to be created to deploy NMS certificate. We will refer to it as "Cisco Medianet NMS Admin" group. The group is created in order to control and limit the number of users that can request a NMS certificate with Administrator role. The members of this group can request a certificate via manual enrollment.
- **Copy of a User Certificate template**. *When you deploy user certificates, you make a copy of the User certificate template and then configure the copy of the template according to your requirements and the instructions in this guide. You will be using a copy rather than the original so that the configuration of the original template is preserved for possible future use* [Deploying Computer and User Certificate].

  The CA uses the copy of the user template to create certificates that can be issued only to the members of the NMS group in Active Directory.
- **Copy of Computer Certificate template.** As done for the user certificate template, you need to make a copy of the Computer Certificate template and configure the copy of template according to your requirements and to the instructions in this guide. In this way the CA can issue certificates to the Computers part of the Domain Computers group.

- **Group Policy**. Once the certificate templates are configured on the CA, a Group Policy is created to perform auto-enrollment for the Computer Certificates. Note that you can either use the default domain policy or create a new policy. This guide assumes that you are using the default domain policy. Note that auto-enrollment is needed only for Computer Certificates. No policy is needed for NMS User Certificates since the enrollment is manual.

4.5.6.4 Deployment Process

The following steps are needed to deploy Computer Certificates for MSI and User Certificates for NMS users:

- Install the AD CS server role as an enterprise root issuing CA as explained in [Core Network Companion Guide: Deploying Server Certificates]. This step is required only if you have not already deployed a CA on your network. Web Enrollment must be installed as well according to the instructions explained in [Setup Certification Authority Web Enrollment].
- Create a group for the NMS with administrator role and add users to the group. Only users belonging to this group are able to request a NMS certificate with administrator role and connect to the MSI. Access to this group should be limited only to the minimum number of users that need to manage the MSI domain-wide.
- Create and configure copies of the computer and user certificate templates and add them to the CA. You can change the name from Copy of Computer Certificate to “Cisco Medianet MSI Template” and from Copy of User Certificate to “Cisco Medianet NMS Admin Template”.
- Manual Enroll an NMS for a Certificate. Auto-enrollment is not enabled to retrieve a certificate for the NMS. Therefore the NMS will need to retrieve it from the Enterprise Root CA with a manual step.
- Configure Group Policy to perform auto-enrollment for the Computer Certificates. Once the policy is created computers part of the domain will automatically enroll for a certificate when Group Policy is refreshed. Note that no steps are needed to deploy the CA certificate, which will be pushed to the Trusted Root Certification Authorities folder in the certificate store for both the Current User and the Local Computer.

4.5.6.5 Deployment detailed steps

The following are the detailed steps needed to deploy certificates to the MSI and the NMS.

4.5.6.5.1 Create a Group for the NMS Admin and associate NMS users to it

This section explains how to create a group in Active Directory and how to associate the NMS users with administrator role to the group. If an NMS user does not exist, you need to first create it. For more information on Users and Groups in Active Directory refer to [Active Directory Domain Services].

To create an NMS Admin group [How to Create a Group in AD]

1. *In Start, Administrative Tools, open Active Directory Users and Computers.*
2. *In Active Directory Users and Computers window, expand* ***<****domain name****>.com***
3. *In the console tree, right-click the folder in which you want to add a new group (ex: Users)*
4. *Click* ***New****, and then click* ***Group****.*
5. *Type the name of the new group. Use a name that you can easily associate with the role or service for which you are creating the group. For example use "****Cisco Medianet NMS Admin****" group.*
6. *In the* ***New Object - Group*** *dialog box, do the following:*
    a. *In* ***Group scope****, click* ***Global scope****.*
    b. *In* ***Group type****, click* ***Security****.*
7. *Click* ***Ok****.*

To Create an NMS User: [Create a new user account]

1. *Open Active Directory Users and Computers.*
2. *In the console tree, right-click the folder in which you want to add a user account.* ***Where?***
    - *Active Directory Users and Computers/domain node/folder*
3. *Point to* ***New****, and then click* ***User****.*
4. *In* ***First name****, type the user's first name*.

5. *In **Initials**, type the user's initials.*

6. *In **Last name**, type the user's last name.*

7. *Modify **Full name** to add initials or reverse order of first and last names.*

8. In User logon name, type the user logon name, select the UPN suffix in the drop-down list, and then click Next.

9. *In **Password** and **Confirm password**, type the user's password, and then select the appropriate password options. Click **Next.***

10. *Verify that the user details are correct, and then click **Finish.***

To associate a user to the group [Add a member to a group]

1. Open Active Directory Users and Computers.

2. *In the console tree, click the folder that contains the group to which you want to add a member.*
   Where?

   - *Active Directory Users and Computers/**domain node/folder that contains the group***

3. *In the details pane, right-click the group, and then click **Properties**.*

4. *On the **Members** tab, click **Add**.*

5. *In **Enter the object names to select**, type the name of the user, group, or computer that you want to add to the group, and then click **OK**.*

Note:

- *To perform this procedure, you must be a member of the Account Operators group, Domain Admins group, or the Enterprise Admins group in Active Directory, or you must have been delegated the appropriate authority.*

- *Review the privileges of the NMS User and the NMS Group in order to be compliant with the policy in your domain. Do not leave un-needed privileges to the NMS user and the NMS group.*

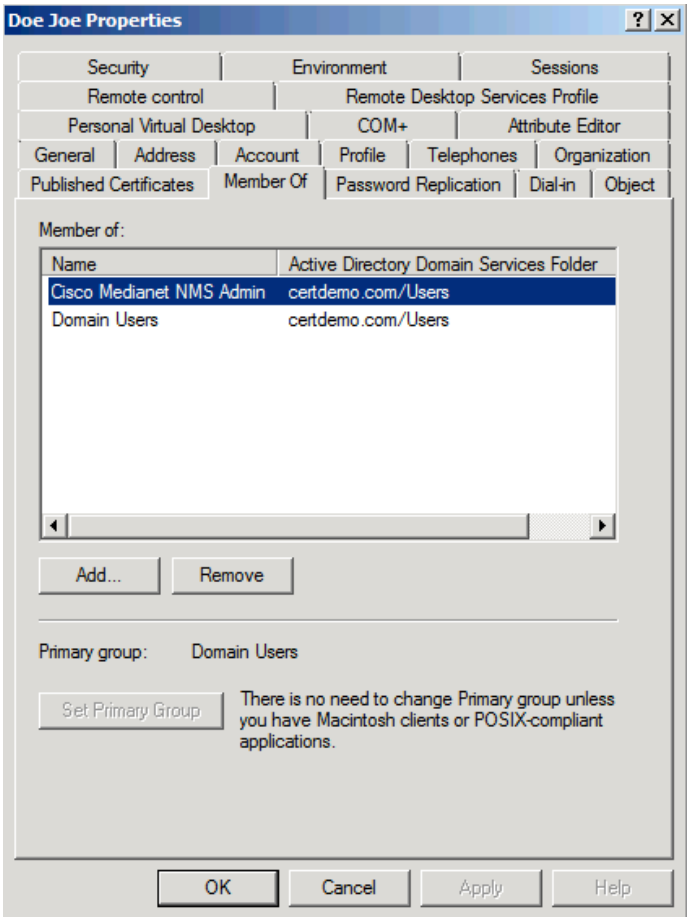


Figure 2: Screenshot of the NMS User member of Cisco Medianet NMS Admin group

4.5.6.5.2 Configure the NMS Admin Certificate Template

This section explains how to use the Microsoft Management Console (MMC) to configure a certificate template to be deployed to the NMS users with administrator role. Reference: [Deploying Computer and User Certificate].

> ***Note**: Membership in both the **Enterprise Admins** and the root domain's **Domain Admins** group is the minimum required to complete this procedure.*

To configure the certificate template and auto-enrollment

1. On the computer where AD CS is installed, click ***Start***, click ***Run***, type **mmc**, and then click ***OK***.
2. On the ***File*** menu, click ***Add/Remove Snap-in***. The ***Add or Remove Snap-ins*** dialog box opens.
3. In the ***Add or Remove Snap-ins*** dialog box, in ***Available snap-ins***, double-click

Certification Authority. Select the certification authority (CA) that you want to manage, and then click ***Finish***. The ***Certification Authority*** dialog box closes, returning you to the ***Add or Remove Snap-ins*** dialog box.

4 In ***Available snap-ins***, double-click ***Certificate Templates***, and then click ***OK***.

5 In the console tree, click ***Certificate Templates***. All of the certificate templates are displayed in the details pane.

6 In the details pane, click the ***User*** template.

7 On the ***Action*** menu, click ***Duplicate Template***. In the ***Duplicate Template*** dialog box, select the template version that is appropriate for your deployment. For client and server interoperability reasons, it is recommended that you select ***Windows Server 2003, Enterprise***. Click ***OK***. The ***Properties of New Template*** dialog box opens.

8 In ***Properties of New Template***, on the ***General*** tab, in ***Display Name***, type a new name for the certificate template: "**Cisco Medianet NMS Admin Template**". In the **Validity** period, write 5 years.

9 In **Subject Name**, **un-tick** E-mail name.

10 In **Subject Name**, un-tick "Include email name in subject name".

11 Click the Request Handling tab. For Minimum key size, determine the best key length for your deployment. It is recommended that you keep the default setting of 2048 bit.

12 Click **Extensions Tab**. Edit **Application Policies**: **Remove** all Application Policies.

13 Edit **Application Policies**: Click **Add.** Select **Client Authentication** and **Server Authentication**. Click **Ok**.

14 In **Application Policies** click **Edit.** Click **Add.** In **Add Application Policy** click **New** and in the **Name** write **"Cisco Medianet MSI NMS admin"** and in the **Object Identifier** write **"1.3.6.1.4.1.9.21.2.2.1.1"** and click **Ok two times and then Apply.**

15 Click the **Security** tab. In **Group or user names**, click **Domain Users**, click **Remove**

16 Click the **Security** tab. In **Group or user names**, click **Add**. Add the "**Cisco Medianet NMS Admin**" group (or the different group name you created earlier). Click **Ok**.

17 In ***Permissions for "Cisco Medianet NMS Admin",*** under ***Allow***, select the **Read, *Enroll*** and then click ***OK***.

18 In the left pane of the Microsoft Management Console (MMC), double-click ***Certification Authority***, double-click the CA name, and then click ***Certificate Templates***. On the ***Action*** menu, point to ***New***, and then click ***Certificate Template to Issue***. The ***Enable Certificate Templates*** dialog box opens.

19 Click the name of the certificate template you just configured "**Cisco Medianet NMS Admin Template**", and then click ***OK***.

Note*: Review carefully the list of certificates that can be issued by your CA. Remove unnecessary certificate templates.*

4.5.6.5.3 Manual Enroll for the NMS Admin Certificate

The NMS can enroll for a User Certificate in several ways according to the different NMS configurations. The following sections cover the various possibilities.

4.5.6.5.3.1 Manual Enroll from a Windows PC with Certificate MMC

If the NMS runs on a Windows PC belonging to the domain, you can follow the following procedure to request a certificate. This procedure refers to a Window 7 PC. For the Windows XP procedure you can refer to [How to Request a Digital Certificate Using MMC].

Note1: You need to be logged in the machine as the NMS user with administrator role.
Note2: The NMS user needs to be member of the "Cisco Medianet NMS Admin" group to request the certificate.

1. Click **Start**, click **Run**, type **certmgr.msc**, and then click **OK**.
2. In MMC, expand **Certificates - Current User**, and then expand **Personal**.
3. In the right pane, right-click and point to **All tasks**, and then click **Request New Certificate**.
4. On the first page of the Certificate Request Wizard, click **Next**.
5. On the **Select Certificate Enrollment Policy**, select **Active Directory Enrollment Policy** and click **Next.**
6. Select **"Cisco Medianet NMS Admin Template"** in the **Certificate types** list, and then click **Enroll**.
7. On the final page of the wizard, click **Finish**.

4.5.6.5.3.2 Manual Enroll from non-Windows Computers

If the user is connecting to the network using a non-Windows computer, for example a Linux or Mac OS X computer, he can enroll for a certificate with a PKCS #10 file and Active Directory Web Enrollment.

Requirements: The current steps assume you have a Web Enrollment installed and running, Mozilla Firefox as a web browser and OpenSSL installed on the machine. For setting up Web Enrollment see [Setup Certification Authority Web Enrollment Support]

4.5.6.5.3.2.1 Create a public key pair and a certificate signing request

1. From the terminal write:

   ```
   openssl req -newkey rsa:2048 -keyout myNMS.key -out myNMS.csr
   ```

2. You will be prompted for a passphrase to protect the private key (***myNMS.key***). The NMS will need this passphrase to be able to use the private key when connecting to MSI.
   Keeping the private key secure is of utmost importance, this is why step 2 will ask you for a passphrase. If on the other hand the private key will reside on a file system with Access Control, and you know what you are doing, you can specify **–nodes** in the previous command to avoid the passphrase.

3. You will be prompted for information that will be added to your certificate request. Press **Enter** to all of them. Pressing Enter leaves the fields with default values.

4. The private key is generated and stored in file ***myNMS.key***. The certificate-signing request is generated in PKCS #10 format and stored in file ***myNMS.csr***.

4.5.6.5.3.2.2 Request a Certificate

References:
[Request a Certificate by Using a PKCS #10 or PKCS #7 File]
[Certificate Enrollment Web Services in Active Directory Certificate Services]

5. *Open a Web browser.*

6. *Open https://**servername**/certsrv, where **servername** is the name of the Web server hosting the CA Web enrollment pages.*

7. If you are prompted for credentials, provide the AD **User Name** and **Password** of the NMS user.

8. *Click **Request a certificate**, and then click **Advanced certificate request**. The page **Submit a Certificate Request or Renewal Request** is displayed.*

9. If you are using a **Linux** terminal, you can install the "**xclip**" utility (e.g **apt-get install xclip**) and then issue:

   ```
   xclip -sel clip < myNMS.csr
   ```

   to copy the contents to the clipboard. If for some reasons you cannot install xclip, then issue:

   ```
   cat myNMS.csr
   ```

   select the output, right click and press **Copy**.

If you are using a **Mac OS X** terminal, you can copy the contents of the CSR to the clipboard using the **pbcopy** command:

```
pbcopy < myNMS.csr
```

10. *On the Web page, click in the **Saved request** box. Right click and then click **Paste** to paste the contents of the certificate request into the box.*

11. *If you are connected to an enterprise CA, choose the certificate template "**Cisco Medianet NMS Admin Template**".*

12. *Click **Submit**.*

13. The **Certificate Issued** Web page appears, select DER or Base64 and click on **Download certificate**. Click on **Save File**.

14. Your certificate is in the Download folder. Move it to the directory as required by the NMS, together with the private key.

Notes:

- *The Web server for the CA must be configured to use HTTPS authentication.*
- *If you submit the request and immediately get a message asking you if you want to submit the request even though it does not contain a BEGIN or END tag, click **OK**.*

***Note**: if the NSM requires the private key and certificate to be stored in a PKCS12 container file, use the following* **openssl** *command:*

```
openssl pkcs12 -export -inkey myNMS.key -in myNMS.cer -out myNMS.p12
```

That command will ask the password to protect the PKCS12 file.

If you don't want to be prompted for the password, you can pass it on the command-line as follows (consider security implications of this):

```
openssl pkcs12 -export -inkey myNMS.key -in myNMS.cer -out myNMS.p12    -pass
MY-SUPER-SECRET-PW
```

File ***myNMS.p12*** will contain both the private key and the certificate, so it is security sensitive.

4.5.6.5.3.2.2.1 Download the CA certificate

Reference [Certification Authority Web Enrollment Guidance]

- *From the web browser, connect to https://<servername>/certsrv, where <servername> is the name of the computer running the CA Web Enrollment role service.*
- *Click **Download a CA certificate, certificate chain, or CRL**.*

- *Select the encoding method that you want to use for the CRL:* ***DER*** *or* ***Base 64****.*
- Under CA Certificate, select the CA certificate that you want to download, and then click Download CA certificate or click Download CA certificate chain. Click on Save File.
- Your CA certificate is in the Download folder. Move it to the directory as required by the NMS configuration.

4.5.6.5.4 Configure the Computer Certificate Template

This procedure is used to configure the "Cisco Medianet MSI Template" based on the default Computer Certificate template. Reference: [Deploying Computer and User Certificate]

Note: *Membership in both the* ***Enterprise Admins*** *and the root domain's* ***Domain Admins*** *group is the minimum required to complete this procedure.*

To configure the certificate template and auto-enrollment

1. *On the computer where AD CS is installed, click* ***Start****, click* ***Run****, type* **mmc***, and then click* ***OK****.*
2. *On the* ***File*** *menu, click* ***Add/Remove Snap-in****. The* ***Add or Remove Snap-ins*** *dialog box opens.*
3. *In the* ***Add or Remove Snap-ins*** *dialog box, in* ***Available snap-ins****, double-click* ***Certification Authority****. Select the CA that you want to manage, and then click* ***Finish****. The* ***Certification Authority*** *dialog box closes, returning you to the* ***Add or Remove Snap-ins*** *dialog box.*
4. *In* ***Available snap-ins****, double-click* ***Certificate Templates****, and then click* ***OK****.*
5. *In the console tree, click the* ***Certificate Templates*** *snap-in. All of the certificate templates are displayed in the details pane.*
6. In the details pane, click the **Computer** template.
7. *On the* ***Action*** *menu, click* ***Duplicate Template****. In the* ***Duplicate Template*** *dialog box, select the template version that is appropriate for your deployment. For client and server interoperability reasons, it is recommended that you select* ***Windows Server 2003 Enterprise****.*
8. *Click* ***OK****. The* ***Properties*** *dialog box for the certificate template opens.*
9. *On the* ***General*** *tab, in* ***Display Name****,* type "**Cisco Medianet MSI Template**". In the **Validity** period, write 5 years.
10. *Click the* ***Subject Name*** *tab. Ensure that* ***Build from this Active Directory information*** *is selected. In* ***Subject name format****, select* ***Fully distinguished name****.*

11. *Click the **Request Handling** tab. For **Minimum key size**, determine the best key character length for your deployment. Large key character lengths provide optimal security, but they can impact server performance. It is recommended that you keep the default setting of 2048.*
12. In the **Request Handling** tab, select **Allow private key to be exported**
13. *Click the **Security** tab. In **Group or user names**, click **Domain Computers**.*
14. *In **Permissions for Domain Computers**, under **Allow**, select the **Enroll** and **Autoenroll** permission check boxes, and then click **OK**.*
15. Click **Extensions Tab**. Edit **Application Policies**: **Remove** all Application Policies except for **Client Authentication** and **Server Authentication**. Click **Ok**.
16. In **Application Policies** click **Edit.** Click **Add.** In **Add Application Policy** click **New** and in the **Name** write **"Cisco Medianet MSI endpoint",** in **Object Identifier** write **"1.3.6.1.4.1.9.21.2.2.2"** and click **Ok 3 times.**
17. **Click Ok one more time to save the changes to the template.**
18. *In the left pane of the Microsoft Management Console (MMC), double-click **Certification Authority**, double-click the CA name, and then click **Certificate Templates**. On the **Action** menu, point to **New**, and then click **Certificate Template to Issue**. The **Enable Certificate Templates** dialog box opens.*
19. *Click the name of the certificate template you just configured, and then click **OK**.*

***Note**: Review carefully the list of certificates that can be issued by your CA. Remove unnecessary certificate templates.*

4.5.6.5.5 Configure Computer Certificate Auto-enrollment

You can use this procedure to automatically enroll, or auto-enroll, client computer certificates to domain member computers. Reference: [Deploying Computer and User Certificate]

***Note:** Membership in both the **Enterprise Admins** and the root domain's **Domain Admins** group is the minimum required to complete this procedure.*

Note**: this procedure assumes that you modify the **Default Domain Policy.** It is possible as well to create a separate group policy object and apply it to the domain with the **Group Policy Manager.

To configure client computer certificate auto-enrollment

1. *On the computer where Active Directory Domain Services (AD DS) is installed, click*

Start**, click **Run**, type* **mmc, and then click **OK**. The Microsoft Management Console (MMC) opens.*

2. *In the MMC, on the **File** menu, click **Add/Remove Snap-in**. The **Add or Remove Snap-ins** dialog box opens.*
3. *In the **Add or Remove Snap-ins** dialog box, in **Available snap-ins**, scroll down to and double-click **Group Policy Management Editor**. The Group Policy Wizard opens.*
4. *In **Select Group Policy Object**, click **Browse**. The **Browse for a Group Policy Object** dialog box opens.*
5. *In **Domains, OUs, and linked Group Policy Objects**, click **Default Domain Policy**, and then click **OK**.*
6. *Click **Finish**, and then click **OK**.*
7. *In the MMC, expand the following path: **Default Domain Policy**, **Computer Configuration**, **Policies**, **Windows Settings**, **Security Settings**, **Public Key Policies**.*
8. *Click **Public Key Policies**, and then in the details pane double-click **Certificate Services Client - Auto-Enrollment**. The **Certificate Services Client - Auto-Enrollment Properties** dialog box opens. Configure the following items, and then click **OK**:*
   a. *In **Configuration Model**, select **Enabled**.*
   b. *Select the **Renew expired certificates, update pending certificates, and remove revoked certificates** check box.*
   c. *Select the **Update certificates that use certificate templates** check box."*

4.5.6.5.6 Auto-Enroll for the Computer Certificates

If the computer has already joined the domain, you can use this procedure to manually refresh Group Policy on the local computer in order to auto-enroll for the certificate. Reference: [Deploying Computer and User Certificate]

***Note:** Group Policy is automatically refreshed when you restart the domain member computer, or when a user logs on to a domain member computer. In addition, Group Policy is periodically refreshed. By default, this periodic refresh is performed every 90 minutes with a randomized offset of up to 30 minutes.*

*Membership in **Administrators**, or equivalent, is the minimum required to complete this procedure.*

To refresh Group Policy on the local computer

1. *Click **Start**, click **Run**, type* **cmd***, and then press ENTER. The Command Prompt window opens.*

2. *Type* **gpupdate***, and then press ENTER.*

If the computer has not yet joined the domain, please add the machine to the AD domain by following the instructions described here Join the computer to the domain

4.5.6.5.7 Verify Computer Certificate Auto-enrollment

In order to verify that the Windows PC auto-enrolled for a Computer Certificate, use the following procedure to verify that your computer certificate is present in the certificate store: (Reference: [How to: view Certificate with the MMC snap-in])

1. *Open a Command Prompt window.*
2. *Type* **mmc** *and press the ENTER key. Note that to view certificates in the local machine store, you must be in the Administrator role.*
3. *On the* ***File*** *menu, click* ***Add/Remove Snap In****.*
4. *Click* ***Add****.*
5. *In the* ***Add Standalone Snap-in*** *dialog box, select* ***Certificates****.*
6. *Click* ***Add****.*
7. *In the* ***Certificates snap-in*** *dialog box, select* ***Computer account*** *and click* ***Next****. Optionally, you can select* ***My User account*** *or* ***Service account****. If you are not an administrator of the computer, you can manage certificates only for your user account.*
8. *In the* ***Select Computer*** *dialog box, click* ***Finish****.*
9. *In the* ***Add Standalone Snap-in*** *dialog box, click* ***Close****.*
10. *On the* ***Add/Remove Snap-in*** *dialog box, click* ***OK****.*
11. *In the* ***Console Root*** *window, click* ***Certificates (Local Computer)*** *to view the certificate stores for the computer.* The computer certificate should be present.

4.5.6.5.8 MSI/MSIREST and Active Directory interaction

Once auto-enrollment is executed, certificates are present locally in the Windows Certificate Store. It is sufficient to install the MSI package to have the management interface up and running with the correct certificate setup. This is the recommended deployment.

If MSIREST is already installed before certificates are present or if it is the first time that the machine is joining the domain, once auto-enrollment is executed MSIREST needs to be restarted. This can be achieved restarting manually the MSIREST service (Reference: Start, stop, resume, restart service) or rebooting the Windows PC (Reference: Restart computers via GPO).

4.5.6.5.9 Certificate revocation list

Each certificate has its own validity period, non-the less its validity can be revoked for several reasons, for instance a suspected compromise of certificate private key or a certificate obtained fraudulently.

In order to make the validity information available to the client, Active Directory Certificate Services publishes a list called certificate revocation list (CRL).

These lists are made available through CRL distribution points that can specify HTTP or LDAP addresses. These lists are published periodically and are retrieved and cached by clients. The CRL is then used to verify that the certificate used by a client is still valid.

The main steps to set up CRL are the following:

1. Specify the CRL Distribution Point
2. Schedule the publication of the CRL
3. Revoke/Un-revoke a certificate

4.5.6.5.9.1 Specify the CRL Distribution Point

The CRL distribution points (CDP) are defined in AD CS and then specified in the issued certificates as a field in the certificate itself. In order to create a CDP and set it in issued certificates, follow this procedure:

1. Configure CDP settings
2. Create a DNS record
3. Configure the IIS web server

Reference: [Creating a Certificate Revocation List Distribution Point for Your Internal Certification Authority]

To configure CDP settings

1. *On the Certificate Authority, open the **Certification Authority** snap-in.*
2. *In the console tree, click the name of the CA.*
3. *On the Action menu, click **Properties**, and then click the **Extensions** tab.*
4. *In **Select** extension, click **CRL Distribution Point**.*
5. *To specify the location for the CRL, click **Add** to open the **Add Location** dialog box.*
6. ***CRL URLs** can be **HTTP** or **LDAP** addresses*

    1. *LDAP: typically defined as **ldap://CN=<CDP CA name variable>,CN=<CDP server variable><other CDP variables>***

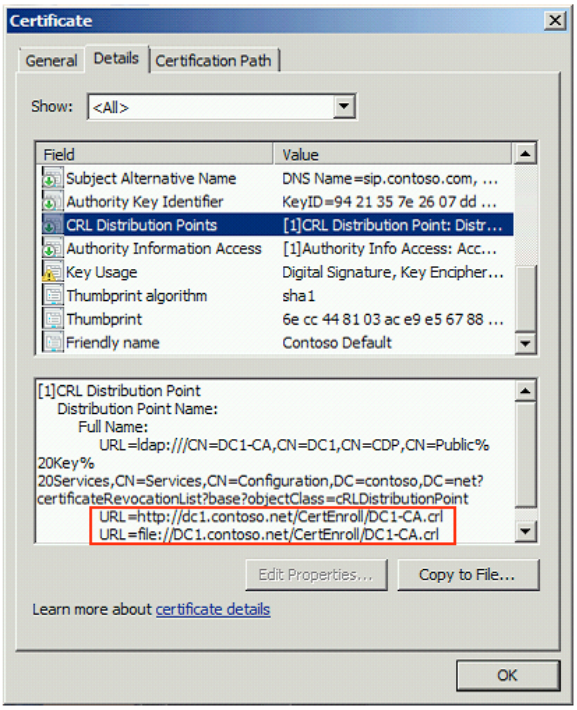
    2. *HTTP/HTTPS – **http://<CA server name>\CertEnroll\<CDP variables>.** You can find the available variables defined here: (Reference: [To specify CRL distribution points in issued certificates])*

7. *Click **OK** to save the location. Repeat to add multiple locations.*
8. *In the **Specify locations list**, click a location, and then select the **Include** in the CRL distribution point extension of issued certificates check box.*
9. *Click **OK** to save changes. **Active Directory Certificate Services** must be restarted for the changes to take effect.*

4.5.6.5.9.2 Configure IIS Web Server

1. *To create the web-based CDP, click **Start**, point to **Administrative Tools**, and then click Internet Information Services (IIS) Manager.*
2. *In the console tree, navigate to FS01\Sites\Default Web Site. Right-click Default Web Site and click **Add** Virtual Directory.*
1. *In the **Add** Virtual Directory dialog box, in Alias, type* **CRLD***. Next to Physical path, click the ellipsis "…" button.*
2. *In the Browse for Folder dialog box, click Local Disk (C:), and then click Make New Folder.*
3. *Type* **CRLDist***, and then press **ENTER**. Click **OK** in the Browse for Folder dialog box.*
4. *Click **OK** in the Add Virtual Directory dialog box.*
5. *In the middle pane of the console, double-click **Directory Browsing**.*
6. *In the details pane, click **Enable**.*
7. *In the console tree, click the CRLD folder.*
8. *In the middle pane of the console, double-click the Configuration Editor icon.*
9. *Click the down-arrow for the Section drop-down list, and then navigate to **system.webServer\security\requestFiltering.***
10. *In the middle pane of the console, double-click the **allowDoubleEscaping** entry to change the value from False to True.*
11. *In the details pane, click Apply.*

Following this configuration a new certificate contains the field CRL Distribution Point as show in the following picture:



For example having defined the CA as “DC1”, and contoso.com the http address, an HTTP and LDAP CDP addresses will look like:

- URL=http://crl.contoso.com/crld/DC1-CA.crl
- URL=ldap:///CN=DC1-CA,CN=DC1,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,contoso,DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint

4.5.6.5.9.3 Schedule publication of the CRL

The publication of the CRL or delta CRL can be scheduled on a regular basis. (Reference: [Schedule Publication of Certificate Revocation Lists])

1. *Open the **Certification Authority** snap-in.*
2. *In the console tree, click **Revoked Certificates**.*
3. *On the **Action** menu, click **Properties**.*
4. *Select the **Publish Delta CRLs** check box*
5. *In **CRL publication interval**, type the increment and click the unit of time to use for the automatic publishing of the CRL. Leave the default values unless required differently.*

4.5.6.5.9.4 Revoke/Un-revoke a certificate

The following procedure describes how to revoke a certificate (Reference: [Manage Certificate Revocation])

1. *Open the **Certification Authority** snap-in.*
2. *In the console tree, click **Issued Certificates**.*
3. *In the details pane, click the certificate you want to revoke.*
4. *On the **Action** menu, point **to All Tasks**, and click **Revoke Certificate**.*
5. *Select the reason for revoking the certificate, adjust the time of the revocation, if necessary, and then click **Yes**.*
6. *To publish it, in the **Certification Authority** snap-in, publish a new CRL by clicking Certification Authority (Computer)/CA name/Revoked Certificates in the console tree. Then, on the **Action** menu, point to **All Tasks**, and click **Publish***

To un-revoke a certificate the following steps are needed:

Note: only certificates that have been revoked with the reason of "Certificate Hold" can be unrevoked.

1. *Open the Certification Authority snap-in.*
2. *In the console tree, click **Revoked Certificates**.*
3. *In the details pane, click the certificate you want to un-revoke.*
4. *On the **Action** menu, point to **All Tasks**, and click **Unrevoke Certificate**.*
5. *Select the reason for un-revoking the certificate, adjust the time of the revocation, if necessary, and then click **Yes**.*

As soon as the certificate has been un-revoked, the CRL needs to be published as done in step 6 before.

5 Deploying Cisco MSI on Mac OS X

The Cisco MSI Runtime package must be predeployed on a Mac OS X user machine for compatible applications to use Cisco MSI services. It is distributed as a Mac OS X installer package (.pkg) and can be installed if needed without any user interaction (Section 5.2: Silent Installation).

The identifier for the package is com.cisco.pkg.CiscoMediaServicesInterface and the files are installed at /Library/Cisco Systems/Media Services Interface.

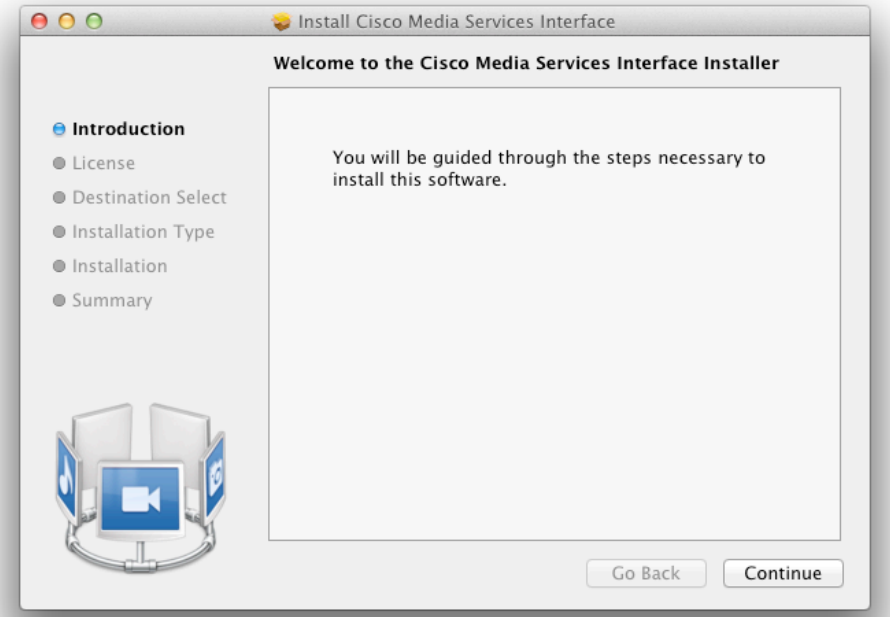
Note that you must have administrative privileges to run the installer.

The component that is installed is the Cisco Media Services Interface daemon, a launch daemon on Mac OS X, started at boot time, which runs under the user "_ciscomsi" account. It is configured to log to the syslog (see the Appendix B: Troubleshooting for more details on logging).

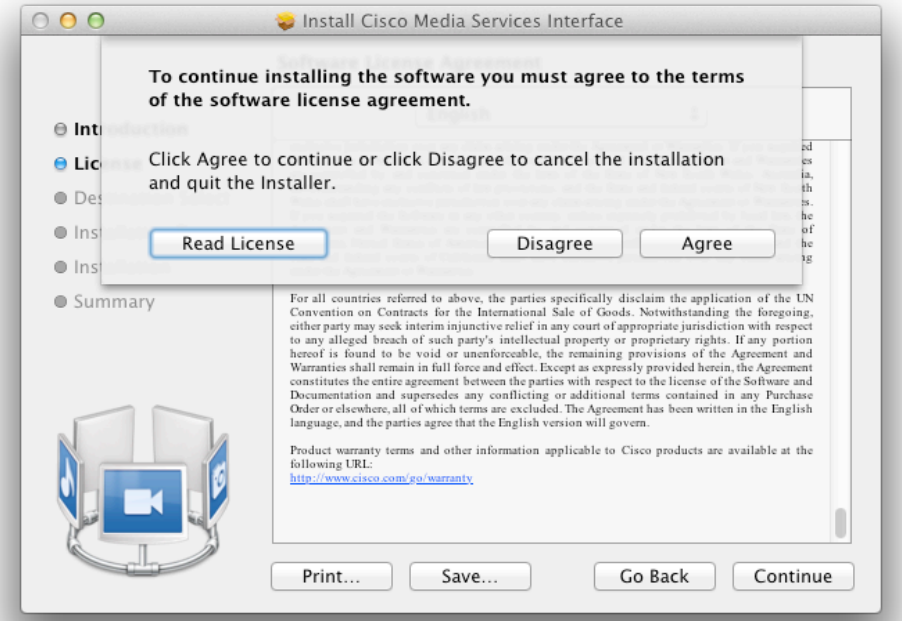
5.1 Manual Installation

To install Cisco MSI on your machine, complete the following steps:

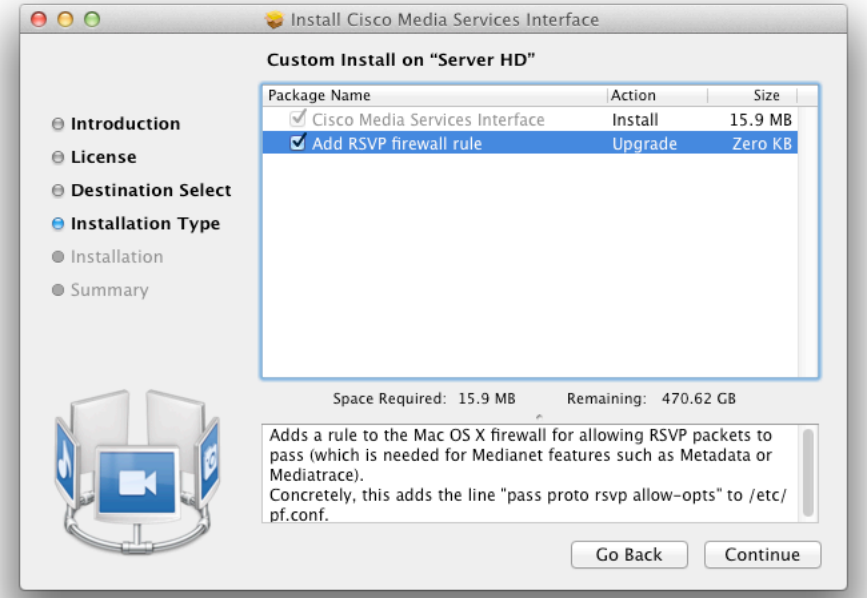
1. Run the MSI installer package (.pkg) and follow the installation wizard.



2. Read and accept the Cisco Media Services License Agreement.



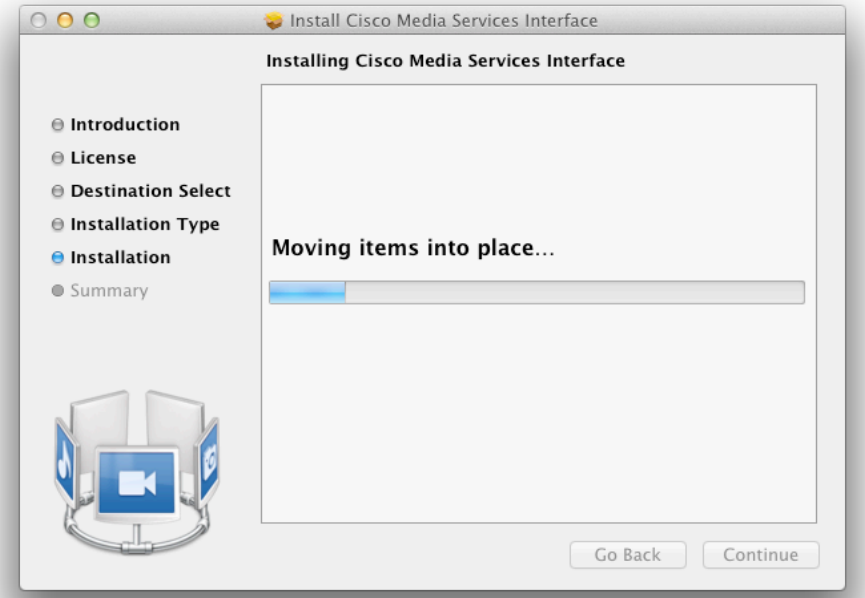
3. Choose **Continue** (recommended) or customize your installation.



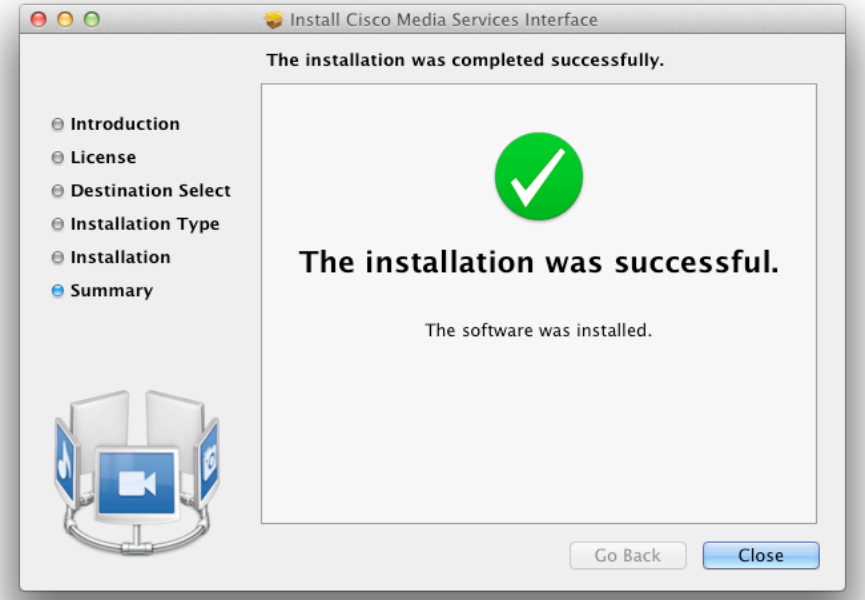
Note that Medianet features such as Metadata or Mediatrace use the Resource Reservation Protocol (RSVP). For Cisco MSI to provide such functionalities, you must

add the RSVP firewall rule to allow incoming RSVP traffic, which is disabled by default by the Mac OS X firewall. Uninstalling Cisco MSI automatically removes this rule.

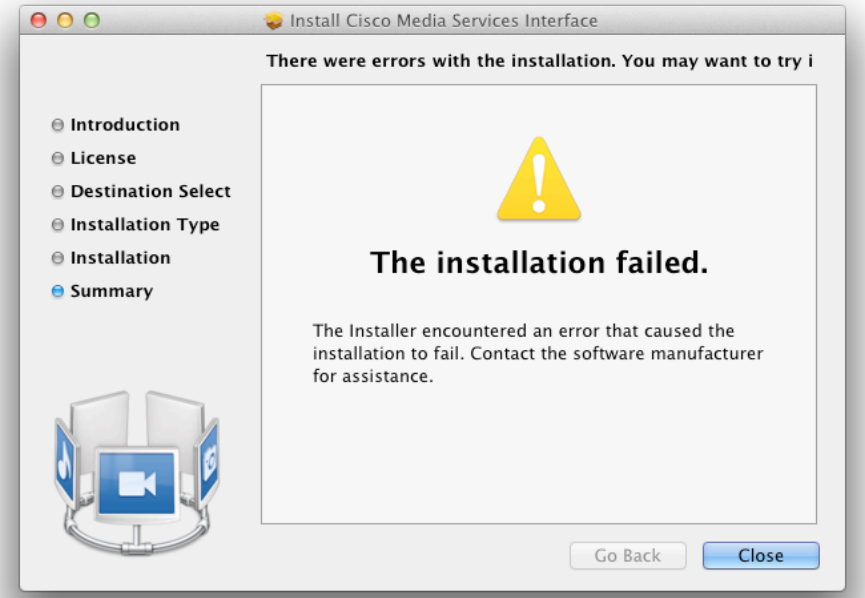
4. Continue to follow the wizard until the installation is completed.



5. If the following dialog box appears, you have successfully installed Cisco MSI. Click **Close** to complete the installation.



6. If the installation fails, the following dialog box appears. See the Appendix B: Troubleshooting for instructions on how to troubleshoot your problem.



5.2 Silent Installation

You can install Cisco MSI silently on Mac OS X, with no user interface and no user interaction. To launch a silent installation, use the Apple installer command-line utility. Run the following command:

```
sudo installer -pkg "Cisco Medianet Services Interface.pkg" -target /
```

Run the **man installer** command for information about how to use the installer from the command line.

5.3 Uninstalling Cisco MSI

To uninstall Cisco MSI, as an administrator, run the following script from the command line:

```
sudo /Library/Cisco\ Systems/Media\ Services\ Interface/uninstaller.py
```

If the Cisco MSI daemon is running, it will be stopped, and all the client applications that are using Cisco MSI will no longer have access to its features.

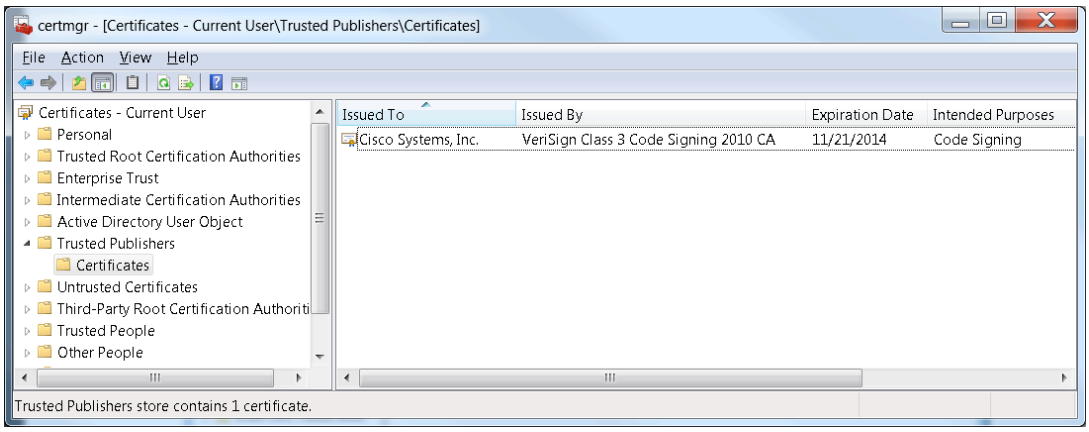
Appendix A: Silent Installation on Windows

When you launch the Cisco MSI installer for the first time on a Windows 7 or 8 machine, a popup confirmation request from Windows Security blocks the silent installation. This popup request concerns the Cisco MSI Protocol Driver that is about to be installed, and it occurs even though the device driver is signed with valid certificates. The solution to this problem requires proper certificate deployment, and this appendix describes the overall approach.

During manual installation, when the Windows Security popup appears and you check the **Always trust** check box, a Cisco certificate is added in the Windows Certificate Store (under Trusted Publishers). Then any further installation on the same machine will first look up for the Cisco certificate, and if it does not find it, a popup appears. However, if you then copy this certificate and add it in the Store of any other Windows 7 or 8 machines prior to installing Cisco MSI, the installation will run silently on them, without asking for permission.

The following steps are an example of how to make sure that you add the right certificate:

1. Install Cisco MSI manually on a machine and be sure to check the **Always Trust** check box when it asks for permission.
2. Get the certificate as follows:
    a. Run **certmgr.msc** at the command prompt.



    b. In the certmgr window, select **Trusted Publishers > Certificates**.
    c. Right-click the Cisco Systems, Inc. certificate and navigate to **All Tasks > Export**.
    d. Follow the Export Wizard, keeping the default settings and selecting a directory in which to save the certificate.

3. Copy this certificate to any machine that you want to run a silent installation on and run, as an administrator, **certutil -addstore "TrustedPublisher"** ***cisco.cer*** at the command prompt (where ***cisco.cer*** is the name of the exported certificate).
4. You can now perform a silent installation of Cisco MSI on any machine on which you copied the certificate.

Note that Windows provides many ways to deploy certificates on several Windows machines at once, especially through Group Policies (see the online Windows documentation).

Appendix B: Troubleshooting

Troubleshooting on Windows

Installer logging

In case of problems during the installation, you can enable detailed logging by installing the package using the following command:

```
msiexec /lv <logfile> /i msi_setup_$version.msi
```

Event Viewer

If you have problems when using Cisco MSI, a detailed log is available in Windows Event Viewer. To access those logs and troubleshoot your problem, follow these steps.

On Windows 7:

1. Open Event Viewer by clicking **Start**. In the Search field, enter **Event Viewe**r, and from the list of results, click **Event Viewer**.
2. From the left menu, double-click **Applications and Services** and select **Cisco MSI** to view the Cisco MSI service logs.
3. From the left menu, double-click **Windows Logs** and select **System** to view the Cisco MSI Protocol Driver logs (only the logs that have **Msidriver** as source).

On Windows XP:

1. Open Event Viewer by choosing **Start > Run**. In the Open field, enter **eventvwr.msc**, and then click **OK**.
2. Choose **Cisco MSI** from the left menu to view the Cisco MSI service logs.
3. Select **System** to view the Cisco MSI Protocol Driver logs (only the logs that have **Msidriver** as source).

You can find more information about how to use the Event Viewer in the online Windows Support page.

Troubleshooting on Mac OS X

Cisco MSI Daemon Logs

Cisco MSI daemon logs are sent to syslog and can be displayed in the Apple Console.app, located at /Applications/Utilities/. The Console application allows you to view the logs that are stored in your Mac.

Installer Logging

The detailed logging of the installation procedure is found in the syslog as well. However, you can redirect these logs to standard error (stderr) if you launch the installation using the Apple installer command-line utility:

```
sudo installer -dumplog -pkg "Cisco Medianet Services Interface.pkg" -target /
```

References

- Medianet: http://www.cisco.com/go/medianet
- Deploying Certificates to the Trusted Publishers Store: http://technet.microsoft.com/en-us/library/cc730989
- How to view and manage event logs in Event Viewer in Windows XP: http://support.microsoft.com/kb/308427
- Windows Server 2008 R2 Core Network Guide (http://www.microsoft.com/en-us/download/details.aspx?id=9166)
- Active Directory Certificate Services (http://technet.microsoft.com/en-us/library/cc772393(v=ws.10).aspx)
- Setup Certification Authority Web Enrollment (http://technet.microsoft.com/en-us/library/cc786960(v=ws.10).aspx)
- Deploying Computer and User Certificate (http://www.microsoft.com/en-us/download/details.aspx?id=7429)
- Core Network Companion Guide: Deploying Server Certificates (http://go.microsoft.com/fwlink/?LinkId=159639)
- How to Create a Group in AD (http://msdn.microsoft.com/en-us/library/aa545347(v=cs.70).aspx)
- Create a new user account (http://technet.microsoft.com/en-us/library/cc784390(v=ws.10).aspx)
- Add a member to a group (http://technet.microsoft.com/en-us/library/cc737130(v=ws.10).aspx#BKMK_winui)
- How to Request a Digital Certificate Using MMC (http://technet.microsoft.com/en-us/library/aa995864(v=exchg.65).aspx)
- Request a Certificate by Using a PKCS #10 or PKCS #7 File (http://technet.microsoft.com/en-us/library/cc770607.aspx)
- Certification Authority Web Enrollment Guidance (http://technet.microsoft.com/en-us/library/hh831649.aspx)
- Join the computer to the domain (http://technet.microsoft.com/en-us/library/cc770919(v=ws.10).aspx)
- How to: view Certificate with the MMC snap-in (http://msdn.microsoft.com/en-us/library/ms788967.aspx)
- [RFC5280] Internet X.509 Public Key Infrastructure Certificate Profile (http://tools.ietf.org/html/rfc5280)
- How to: view Certificate with the MMC snap-in (http://msdn.microsoft.com/en-us/library/ms788967.aspx)

- Creating a Certificate Revocation List Distribution Point for Your Internal Certification Authority (http://blogs.technet.com/b/nexthop/archive/2012/12/17/creating-a-certificate-revocation-list-distribution-point-for-your-internal-certification-authority.aspx)
- Specify CRL Distributions Points (http://technet.microsoft.com/en-us/library/cc753296.aspx)
- Manage Certificate Revocation (http://technet.microsoft.com/en-us/library/cc753724.aspx)
- Schedule Publication of Certificate (http://technet.microsoft.com/en-us/library/cc732174.aspx)