



Secure Internet Traffic



COMPANYCRYPT®
The encryption module for MIMesweeper

Installation Guide
CompanyCRYPT v1.5.0

Installation Guide

CompanyCRYPT v1.5.0

© S.I.T. GmbH & Co. KG

Kaiser-Wilhelm-Str. 9 • 30159 Hanover • Germany

Telefon: +49 511 8999 710 • Telefax: +49 511 8999 712

Internet: www.companycrypt.com • eMail: info@companycrypt.com

© Copyright 2005-2014 by S.I.T. GmbH & Co. KG

Subject to change

The materials contained herein are the sole property of S.I.T.. No part of this publication may be reproduced or disseminated or transmitted in any form or by any means electronic, mechanical, photocopying, recording, or otherwise stored in any retrievable system or otherwise used in any manner whatsoever without the express permission of S.I.T..

S.I.T. provides this publication in the form „as is“ and does not take any liability for this documentation. The non liability includes expressed or implicit guarantees or suitability for defined purposes. The reader or user carries full responsibility for any usage of the information provided in this documentation.

Under no condition shall S.I.T. be liable for any direct or indirect, coincidental, special or resulting damage or loss, derived from any error within or related to the provided information, even and especially when the possibility of loss or damage was stated.

Furthermore S.I.T. claims the right to change, modify, nullify or update this documentation at any given time without the obligation to inform persons or organisations.

The usage of the software related to this documentation is part of and regulated by the licence agreement of S.I.T..

Trademarks

MIMesweeper and MAILsweeper are registered trademark (TM) of the company CLEARSWIFT.

CompanyCRYPT is a registered trademark (TM) of the company S.I.T. GmbH & Co. KG.

Any other trademark, brand, product names or logo not named above but used in this documentation is to be considered a registered trademark of the registered trademark holder.



1 Content

1.1 List of content

1	Content	2
1.1	List of content	2
1.2	Document content	3
2	Preparing the installation	4
2.1	System requirements	4
2.2	Special requirements	4
3	CompanyCRYPT Installation	5
3.1	Choosing the right implementation sequence	5
3.1.1	Installation Sequence 1 – Single Server.....	5
	Installing the program files	6
3.1.2	Installation Sequence 2 – Multiple Server (A)	6
	Installing the program files on the Master System (PCS)	7
	Installing the program files on the Slave System (PS).....	9
3.1.3	Installation Sequence 3 – Multiple Server (B)	10
	Installing the program files on the Slave System (PS).....	11
	Installing the program files on the Master System (PCS)	13
3.2	Installing the WebGUI under Microsoft® Windows Server 2003	15
3.2.1	Setting up the CC-WebGUI as a Virtual Directory.....	15
3.2.2	Setting up Authentication.....	19
3.2.3	Setting up Access Control	20
3.2.4	Activating SSL encryption (optional, recommended)	21
3.2.5	Setting up the URL for Certificate Revocation List – CRL.....	24
3.3	Installing the WebGUI under Microsoft® Windows Server 2008 / 2008 R2	27
3.3.1	Setting up the CC-WebGUI as a Virtual Directory.....	28
3.3.2	Setting up Authentication.....	31
3.3.3	Setting up Access Control	31
3.3.4	Activating SSL encryption (optional, recommended)	33
3.3.5	Setting up the URL for Certificate Revocation List – CRL.....	36
3.4	Installing the WebGUI under Microsoft® Windows Server 2012 / 2012 R2	38
3.4.1	Setting up the CC-WebGUI as a Virtual Directory.....	38
3.4.2	Setting up Authentication.....	42
3.4.3	Setting up Access Control	43
3.4.4	Activating SSL encryption (optional, recommended)	45
3.4.5	Setting up the URL for Certificate Revocation List – CRL.....	48
4	De-installing CompanyCRYPT	51
4.1	Deleting CompanyCRYPT services and EXE.INI entries	51



4.2	Remove CompanyCRYPT program files under Microsoft® Windows Server 2003....	51
4.3	Remove CompanyCRYPT program files under Microsoft® Windows Server 2008 / 2008 R2.....	52
4.4	Remove CompanyCRYPT program files under Microsoft® Windows Server 2012 / 2012 R2.....	52
4.5	Remove CompanyCRYPT-WebGUI under Microsoft® Windows Server 2003	52
4.6	Remove CompanyCRYPT-WebGUI under Microsoft® Windows Server 2008 / 2008 R2	53
4.7	Remove CompanyCRYPT-WebGUI under Microsoft® Windows Server 2008 / 2008 R2	54

1.2 Document content

This document describes the necessary steps to install CompanyCRYPT® on a system with defined preliminaries. It supports you while setting up an operational *CompanyCRYPT®* installation including the administrative access. The configuration of *CompanyCRYPT®* and the integration into the product *MIMESweeper for SMTP®* by *Clearswift®* is described in a separate document named *Configuration Guide*.



2 Preparing the installation

2.1 System requirements

Software:	<p>Microsoft® Windows Server 2003, Microsoft® Windows Server 2008, Microsoft® Windows Server 2008 R2, Microsoft® Windows Server 2012, Microsoft® Windows Server 2012 R2, IIS (Internet Information Server), MIMESweeper for SMTP 5.x</p> <p>The freely available Open Source products GnuPG and OpenSSL are part of the Company-CRYPT installation package.</p>
Hardware:	<p>The same requirements as for the MIMESweeper for SMTP apply. Beyond that:</p> <ul style="list-style-type: none">• CPU > 2 GHz recommended• 100 MB HDD space
Network:	<p>If using synchronisation between multiple CompanyCRYPT installations, a single configurable IP-port (default: 23499) has to be opened between the assigned <i>Master</i> system and each <i>Slave</i> system in both directions.</p>
Permissions:	<p>The installation of CompanyCRYPT has to be done with 'Local Administrator' permissions. Please ensure, that your log-on account meets this requirement or that your account has sufficient permissions to install services and write access to the registry.</p>

2.2 Special requirements

If this install package comes with an additional ReadMe file, please make sure that you have read this before you start the installation. It will contain additional instruction or descriptions of additional requirements.



3 CompanyCRYPT Installation

3.1 Choosing the right implementation sequence

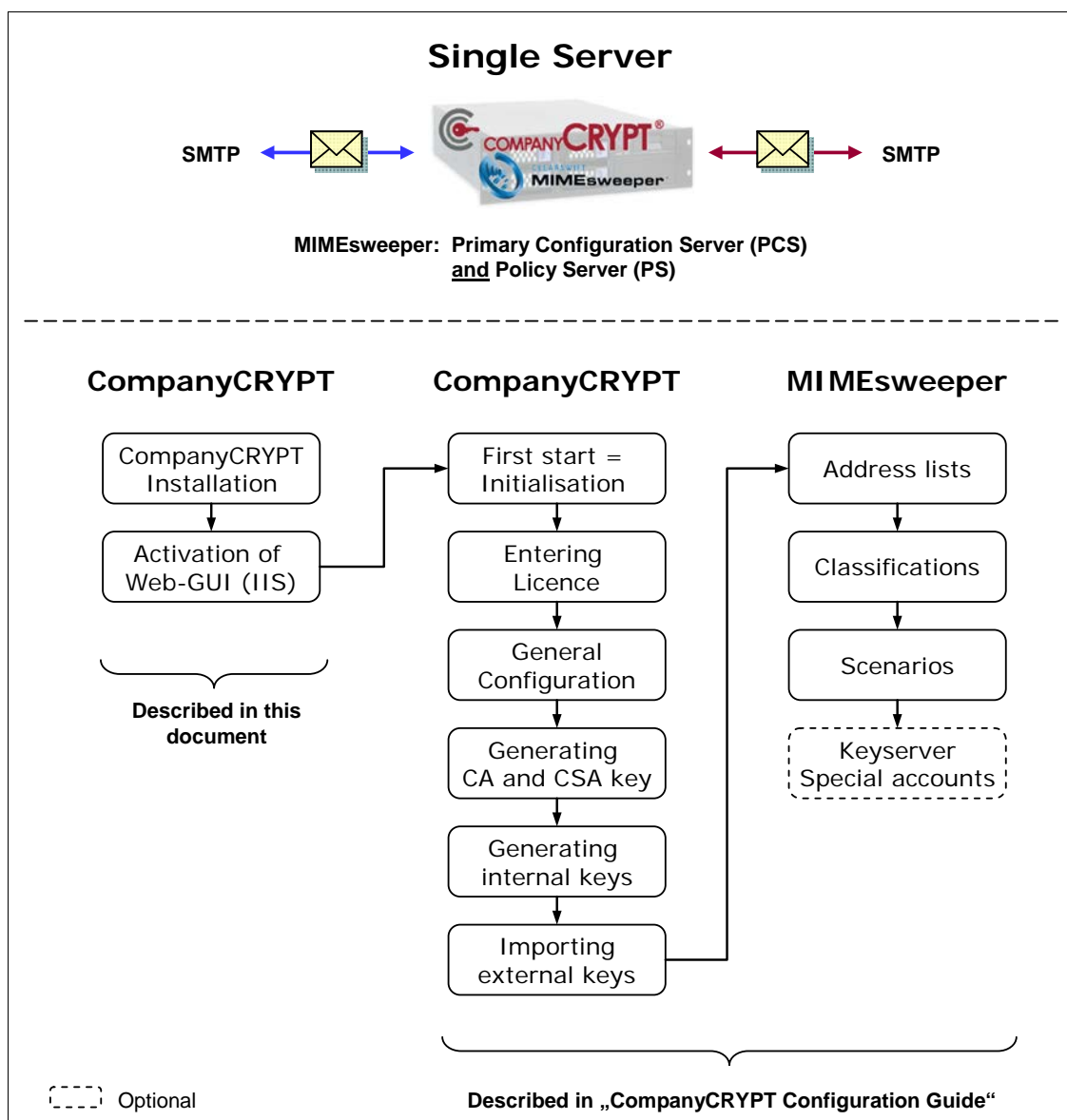
CompanyCRYPT supports MIMESweeper distributed environments with multiple server. CompanyCRYPT key material, data and configuration information can be synchronized across an IP connection. The synchronisation is based on a master-slave model in which the master is used to administrate the CompanyCRYPT deployment centrally.

The next pictures show different outlines of the full CompanyCRYPT implementation (installation and configuration). Depending on the type of MIMESweeper deployment (PCS with/without PS on the same system), the CompanyCRYPT implementation sequence varies. Use the pictures below to select the implementation sequence that matches your MIMESweeper deployment.

Note: The step CompanyCRYPT-“First Start..”, and all following steps (“Entering Licence”) as well as all steps within MIMESweeper are described in the CompanyCRYPT *Configuration Guide*.

3.1.1 Installation Sequence 1 – Single Server

Follow this sequence, if all components are installed on a single server.





Secure Internet Traffic



COMPANYCRYPT®
The encryption module for MIMESweeper

Installation Guide
CompanyCRYPT v1.5.0

Installing the program files

Step 1

Start the installation by a right-click on the file CompanyCRYPT_vXXX_setup.exe („XXX“ stands for the program version) and select **Run as administrator**.

Step 2

The welcome window will appear, click on Next.

Step 3

In the dialog box 'Software-Licence-Agreement' select „I accept ...“ and click on Next.

Step 4

In the next dialog box the target installation directory can be selected. Either proceed with the pre-selected directory with Next or click on the button Change and select the desired directory. Confirm the change by clicking on OK then.

Step 5

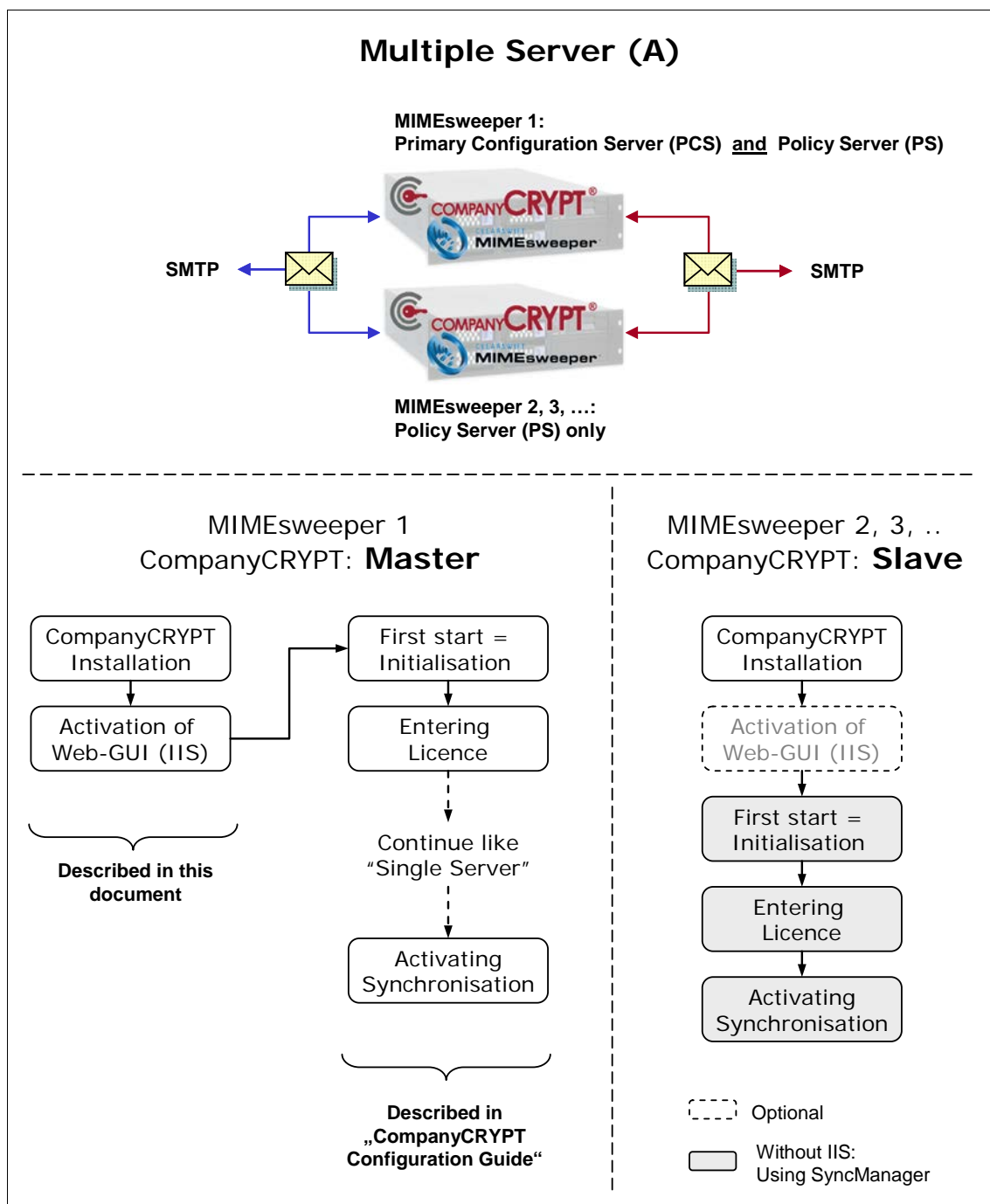
Now by clicking on Install, the program installation will be started. A progress bar will be displayed.

Step 6

A successful installation will be displayed by the window 'Completing the CompanyCRYPT Setup Wizard'. Deactivate the option **Launch CompanyCRYPT**. By clicking on the button **Finish** the process is complete.

3.1.2 Installation Sequence 2 – Multiple Server (A)

Follow this sequence, if your MIMESweeper is a *Primary Configuration Server* (PCS) and a *Policy Server* (PS) is installed and active on the same system. The setup of *Master* and *Slave* can be done independently, it is recommended to start with the *Master*.



Installing the program files on the Master System (PCS)

Step 1

Start the installation by a right-click on the file CompanyCRYPT_vXXX_setup.exe („XXX“ stands for the program version) and select **Run as administrator**.

Step 2

The welcome window will appear, click on Next.

Step 3

In the dialog box 'Software-Licence-Agreement' select „I accept ...“ and click on Next.



Step 4

In the next dialog box the target installation directory can be selected. Either proceed with the pre-selected directory with Next or click on the button Change and select the desired directory. Confirm the change by clicking on OK then.

Step 5

Now by clicking on Install, the program installation will be started. A progress bar will be displayed.

Step 6

A successful installation will be displayed by the window 'Completing the CompanyCRYPT Setup Wizard'. The option **Launch CompanyCRYPT** should be marked. By clicking on the button **Finish** the SyncManager will be started.

Step 7

Within the LICENCE-STATUS frame click on **Add**.

LICENCE-STATUS

NONE - Please enter a licence.

Add

Step 8

Enter your licence details, click on **Apply** and close the window by clicking on **Close**. A valid licence is displayed with a green OK.

CompanyCRYPT Licence

STATUS

CompanyCRYPT Licence: **NONE**

MIMesweeper serial: 4045-0209-1335-6000

Company: Company Name

Serial: Serial Number

Licence-Key: Licence Key

User:

Valid until:

Apply Close

LICENCE-STATUS

VALID - OK

Edit

Step 9

Within the CONFIGURATION frame select **This Server acts as: Master**. Select **Password Source: Manual** and enter a password for synchronisation into the field **Manual Password**. Example: companycrypt

CONFIGURATION

This Server acts as: Master Password Source: Manual

Use Port: 23499 Manual Password: companycrypt

Sync Interval (sec): 30

Below **Valid Sync Host** enter the IP addresses or the DNS names of the Slave systems. Save the settings by clicking on **Apply**.



Valid Sync Hosts	Last Status	Last Connect
slave-host.domain.com	Unknown	Unknown

Apply

Step 10

Start the Operational Service by clicking on the button **Start Service**.

OPERATIONAL-SERVICE
STOPPED - Synchronisation Suspended
Start Service

OPERATIONAL-SERVICE
RUNNING - Synchronisation Active
Stop Service

The synchronisation will automatically commence as soon as the Slave systems have been configured.

Installing the program files on the Slave System (PS)

Step 1

Start the installation by a right-click on the file CompanyCRYPT_vXXX_setup.exe („XXX“ stands for the program version) and select **Run as administrator**.

Step 2

The welcome window will appear, click on Next.

Step 3

In the dialog box 'Software-Licence-Agreement' select „I accept ...“ and click on Next.

Step 4

In the next dialog box the target installation directory can be selected. Either proceed with the pre-selected directory with Next or click on the button Change and select the desired directory. Confirm the change by clicking on OK then.

Step 5

Now by clicking on Install, the program installation will be started. A progress bar will be displayed.

Step 6

A successful installation will be displayed by the window 'Completing the CompanyCRYPT Setup Wizard'. The option **Launch CompanyCRYPT** should be marked. By clicking on the button **Finish** the SyncManager will be started.

Step 7

Within the LICENCE-STATUS frame click on **Add**.

LICENCE-STATUS
NONE - Please enter a licence.
Add

Step 8

Enter your licence details, click on **Apply** and close the window by clicking on **Close**. A valid licence is displayed with a green OK.



CompanyCRYPT Licence

STATUS

CompanyCRYPT Licence: **NONE**

MIMESweeper serial: 4045-0209-1335-6000

Company:

Serial:

Licence-Key:

User:

Valid until:

Apply

Close

LICENCE-STATUS

VALID - OK

Edit

Step 9

Within the CONFIGURATION frame select **This Server act as: Slave**. Select **Password Source: Manual** and enter the password for synchronisation into the field **Manual Password**. Example: companycrypt

CONFIGURATION

This Server acts as:

Password Source:

Use Port:

Manual Password:

Sync Interval (sec):

Below **Valid Sync Host** enter the IP address or the DNS name of the Master system. Save the settings by clicking on **Apply**.

Valid Sync Hosts	Last Status	Last Connect
master-host.domain.com	SYNC OK	2008-01-15 15:03:31
<input type="text"/>		
<input type="text"/>		
<input type="text"/>		

Apply

Step 10

Start the Operational Service by clicking on the button **Start Service**.

OPERATIONAL-SERVICE

STOPPED - Synchronisation Suspended

Start Service

OPERATIONAL-SERVICE

RUNNING - Synchronisation Active

Stop Service

The synchronisation will automatically commence as soon as the Master system becomes available.

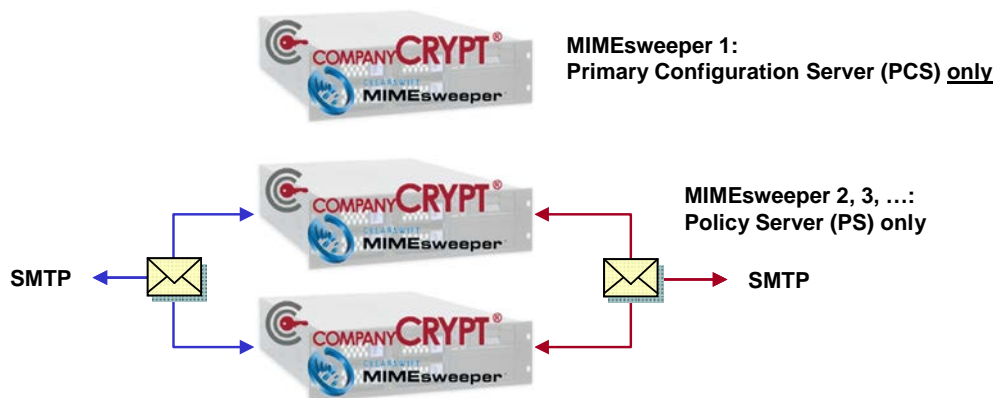
3.1.3 Installation Sequence 3 – Multiple Server (B)

Follow this sequence, if your MIMESweeper is 'only' a *Primary Configuration Server (PCS)* and no *Policy Server (PS)* is active on the same system.

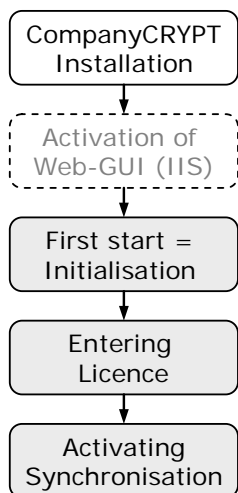
Important: In this sequence it is necessary to set up the slave system first. Only after a successful synchronisation will you be able to access all parts of the WebGUI on the Master system.



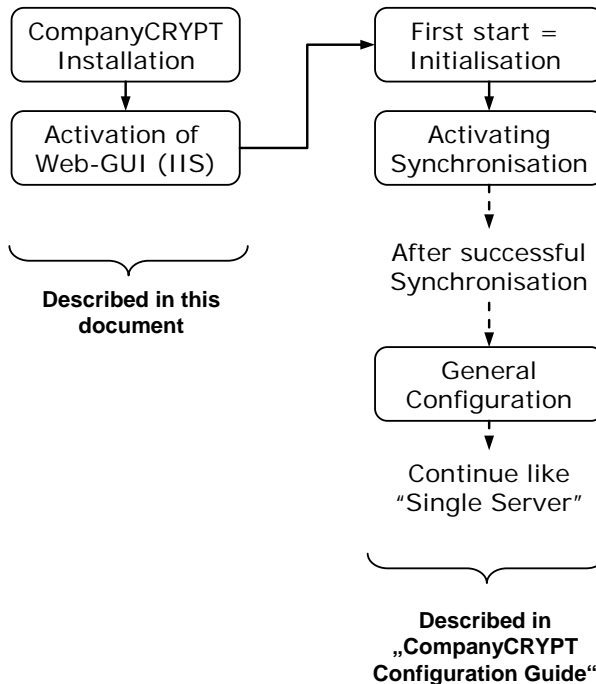
Multiple Server (B)



MIMESweeper 2, 3, .. CompanyCRYPT: **Slave**



MIMESweeper 1 CompanyCRYPT: **Master**



Installing the program files on the Slave System (PS)

Step 1

Start the installation by a right-click on the file CompanyCRYPT_vXXX_setup.exe („XXX“ stands for the program version) and select **Run as administrator**.

Step 2

The welcome window will appear, click on Next.

Step 3

In the dialog box 'Software-Licence-Agreement' select „I accept ...“ and click on Next.

Step 4

In the next dialog box the target installation directory can be selected. Either proceed with the pre-selected directory with Next or click on the button Change and select the desired directory. Confirm the change by clicking on OK then.

Step 5

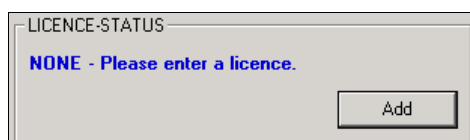
Now by clicking on Install, the program installation will be started. A progress bar will be displayed.

Step 6

A successful installation will be displayed by the window 'Completing the CompanyCRYPT Setup Wizard'. The option **Launch CompanyCRYPT** should be marked. By clicking on the button **Finish** the SyncManager will be started.

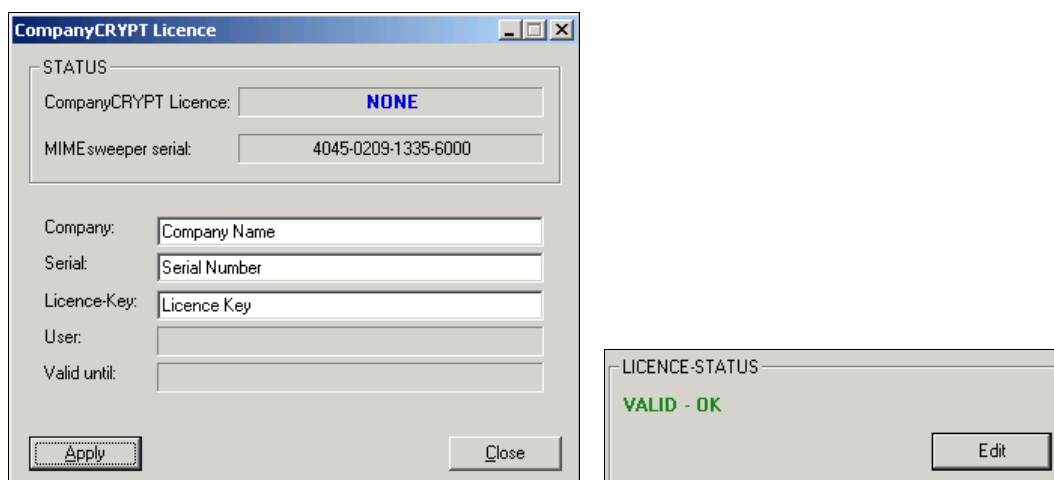
Step 7

Within the LICENCE-STATUS frame click on **Add**.



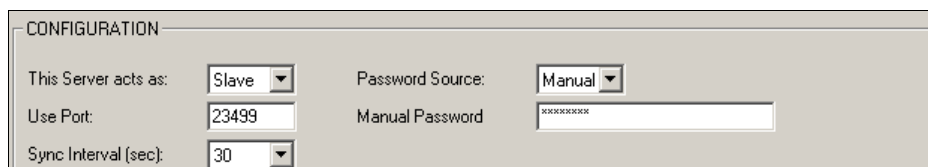
Step 8

Enter your licence details, click on **Apply** and close the window by clicking on **Close**. A valid licence is displayed with a green OK.



Step 9

Within the CONFIGURATION frame select **This Server act as: Slave**. Select **Password Source: Manual** and enter a password for synchronisation into the field **Manual Password**. Example: companycrypt



Below **Valid Sync Host** enter the IP address or the DNS name of the Master system. Save the settings by clicking on **Apply**.

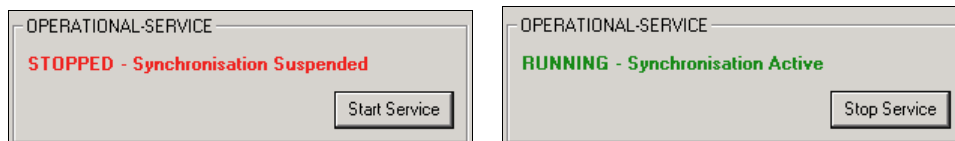


Valid Sync Hosts	Last Status	Last Connect
master-host.domain.com	SYNC OK	2008-01-15 15:03:31

Apply

Step 10

Start the Operational Service by clicking on the button **Start Service**.



The synchronisation will automatically commence as soon as the Master system becomes available.

Installing the program files on the Master System (PCS)

Step 1

Start the installation by a right-click on the file CompanyCRYPT_vXXX_setup.exe („XXX“ stands for the program version) and select **Run as administrator**.

Step 2

The welcome window will appear, click on Next.

Step 3

In the dialog box 'Software-Licence-Agreement' select „I accept ...“ and click on Next.

Step 4

In the next dialog box the target installation directory can be selected. Either proceed with the pre-selected directory with Next or click on the button Change and select the desired directory. Confirm the change by clicking on OK then.

Step 5

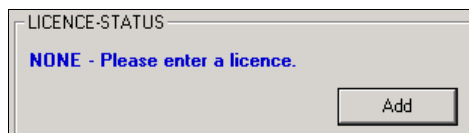
Now by clicking on Install, the program installation will be started. A progress bar will be displayed.

Step 6

A successful installation will be displayed by the window 'Completing the CompanyCRYPT Setup Wizard'. The option **Launch CompanyCRYPT** should be marked. By clicking on the button **Finish** the SyncManager will be started.

Step 7

Within the LICENCE-STATUS frame click on **Add**.



Step 8

Enter your licence details, click on **Apply** and close the window by clicking on **Close**. A valid licence is displayed with a green OK.



CompanyCRYPT Licence

STATUS

CompanyCRYPT Licence: **NONE**

MIMESweeper serial: 4045-0209-1335-6000

Company:

Serial:

Licence-Key:

User:

Valid until:

LICENCE-STATUS

NOT VALID - Please enter a valid licence.

Step 9

Within the CONFIGURATION frame select **This Server acts as: Master**. Select **Password Source: Manual** and enter the password for synchronisation into the field **Manual Password**. Example: companycrypt

CONFIGURATION

This Server acts as: Password Source:

Use Port: Manual Password:

Sync Interval (sec):

Below **Valid Sync Host** enter the IP addresses or the DNS names of the Slave systems. Save the settings by clicking on **Apply**.

Valid Sync Hosts	Last Status	Last Connect
slave-host.domain.com	Unknown	Unknown

Step 10

Start the Operational Service by clicking on the button **Start Service**.

OPERATIONAL-SERVICE

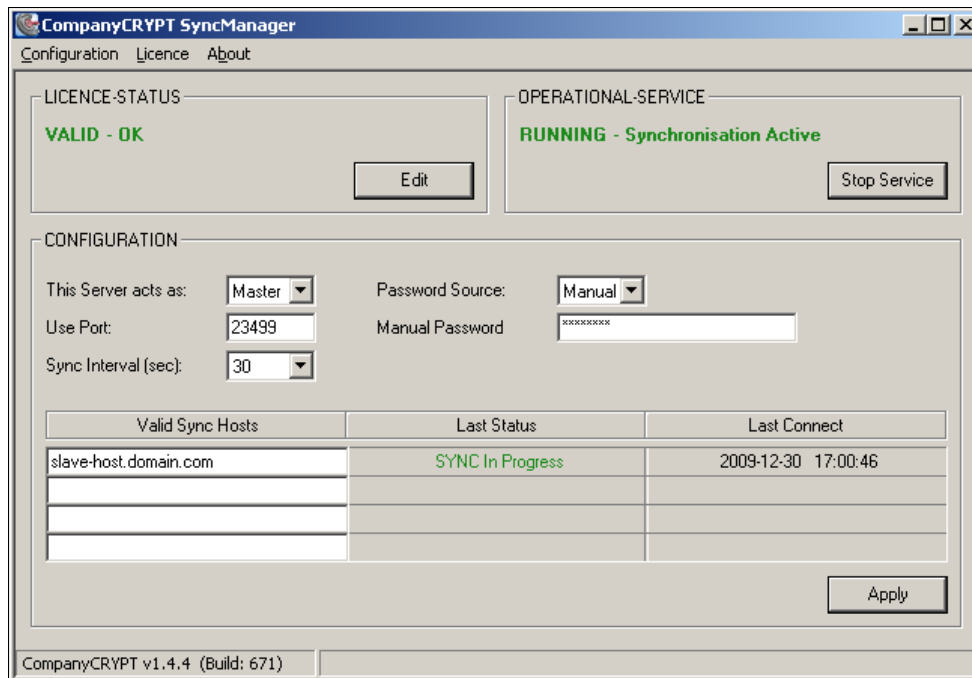
STOPPED - Synchronisation Suspended

OPERATIONAL-SERVICE

RUNNING - Synchronisation Active

Step 11

The synchronisation will automatically commence as soon as the Slave system has been configured. During the first synchronisation cycle the licence information will be validated.



3.2 Installing the WebGUI under Microsoft® Windows Server 2003

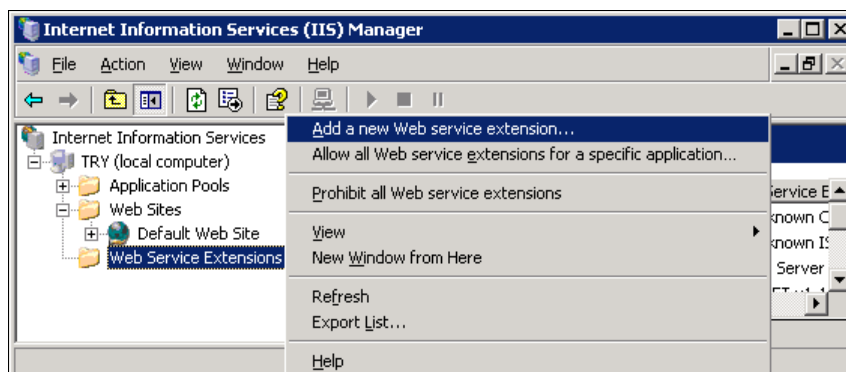
The following pages will describe the integration into a Microsoft® Internet Information Service (IIS) 6.0 under Windows Server 2003®. Upon integration into an older version of the IIS (or MS-Windows) the name of some paths and menu items may differ from the documented information hereafter.

3.2.1 Setting up the CC-WebGUI as a Virtual Directory

The implementation as a Virtual Directory is highly recommended. It means that when accessing the CompanyCRYPT-WebGUI, the address consists of the domain (of the hostname) and the selected directory for CompanyCRYPT. Example: mail.host.com/CCWEB

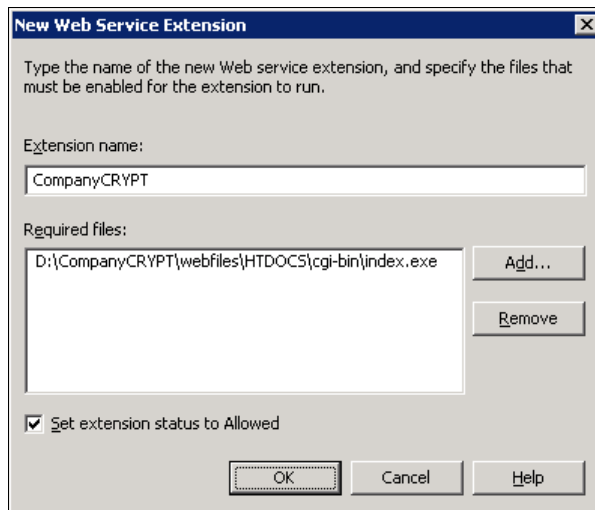
Step 1

Move to and right-click on **Internet Information Services** → ... (Local Computer) → **Web Sites** → **Web Service Extensions** and select **Add a new Web service extension**.



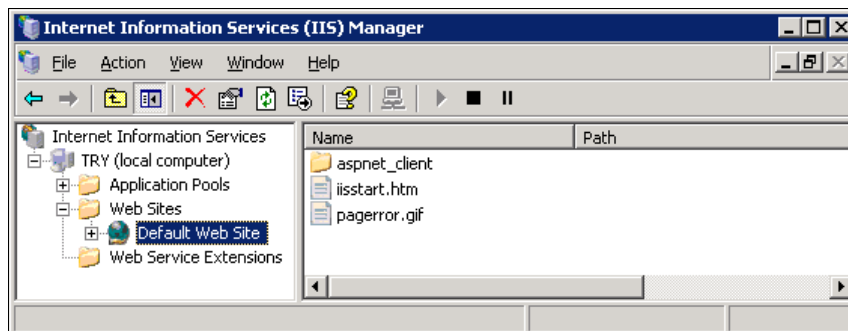
Step 2

Enter **CompanyCRYPT** into the field **Extension Name**. Now click on **Add...** and add to the file **<CompanyCRYPT-Install directory>\Webfiles\IHTDOCS\cgi-bin\index.exe**. Finally activate the field **Set extension status to Allowed**.



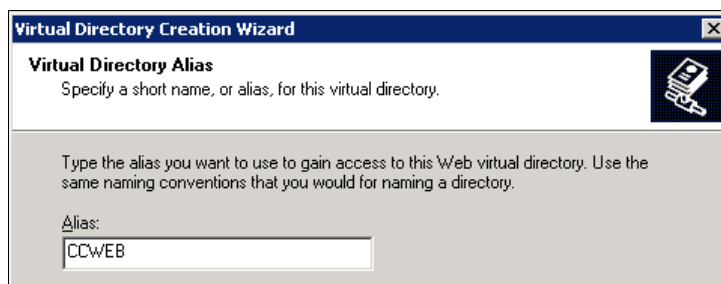
Step 3

Begin with **Start → All Programs → Administrative Tools** and start the **Internet Information Services (IIS) Manager**. Move to **Internet Information Services → ... (Local Computer) → Web Sites** and select **Default Web Site**.



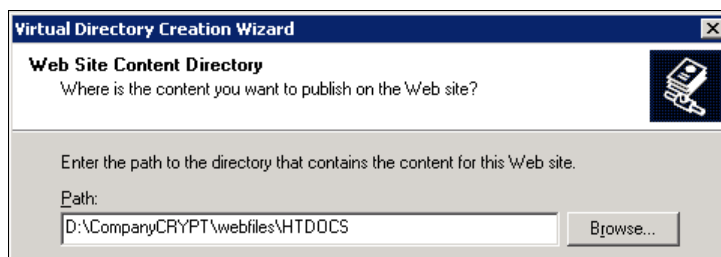
Step 4

Right-click on **Default Web Site** and select **New → Virtual Directory**. Enter **CCWEB** as an alias or choose an individual name.



Step 5

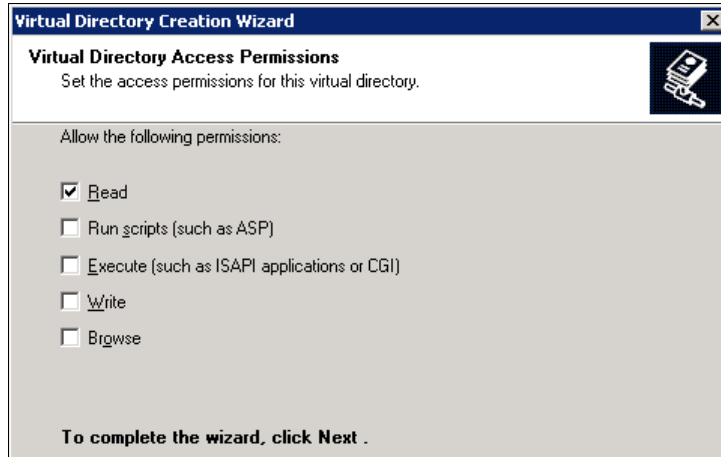
Enter the following path according to your installation: **<CC-Install directory>\Webfiles\HTDOCS**





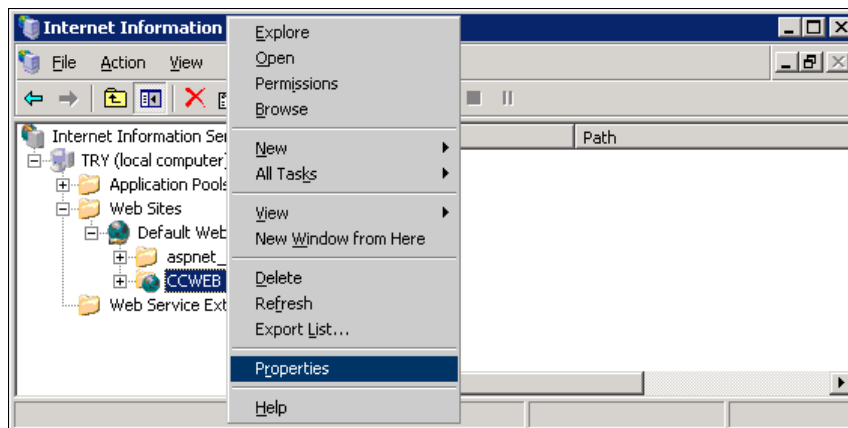
Step 6

Under permissions only mark **Read**.



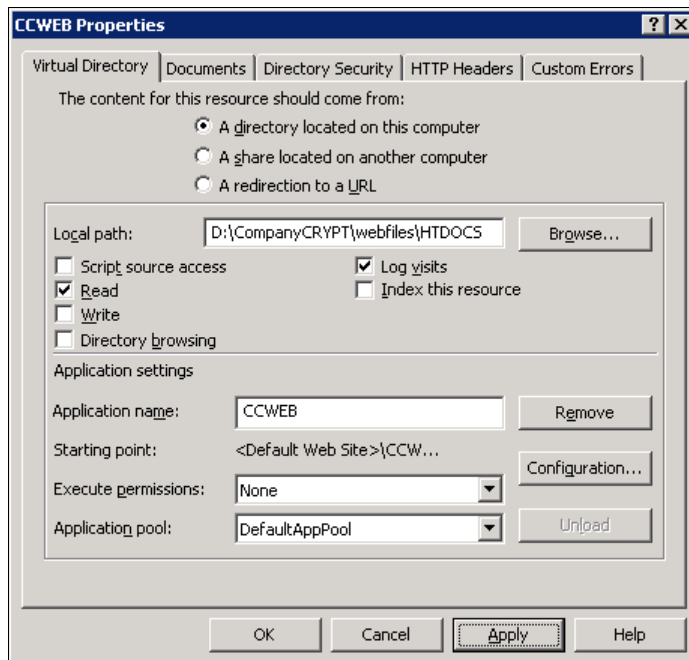
Step 7

Right-click on **Internet Information Services** → ... (Local Computer) → **Web Sites** → **Default Web Site** → **CCWEB** and select **Properties**.



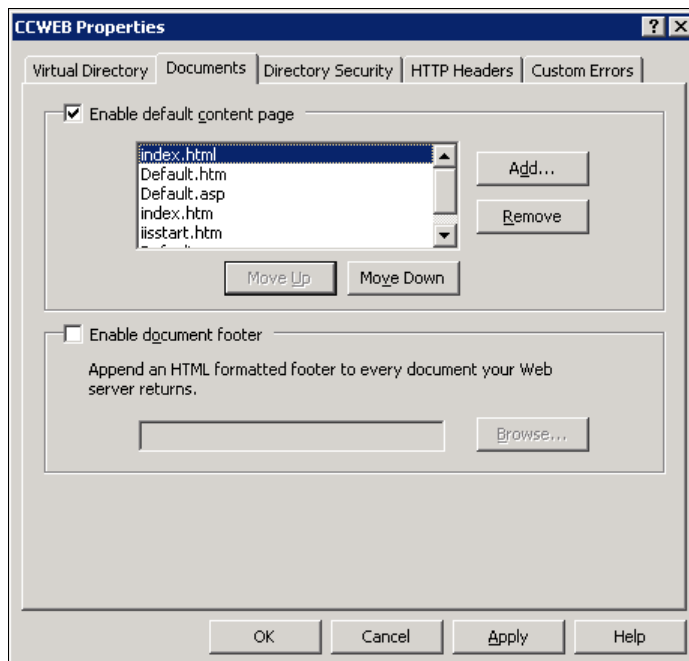
Step 8

In the properties window select the tab **Virtual Directory**. Now mark the permission **Read**, deactivate **Index this resource** and select under **Execute permissions:** **None**. If the field **Application name** is empty, click on **Create** and enter **CCWEB**.



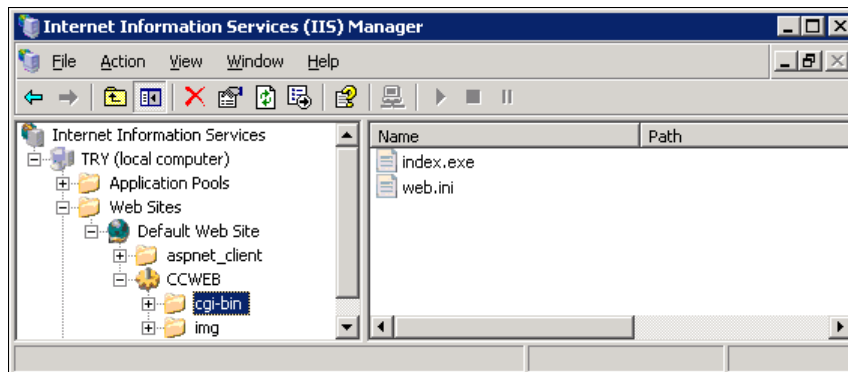
Step 9

Continue in the properties window and move to **Documents**. Activate the option **Enable default content page**. Add the file name **index.html** and move it to the top of the list. Save all setting by leaving this window with **OK**.



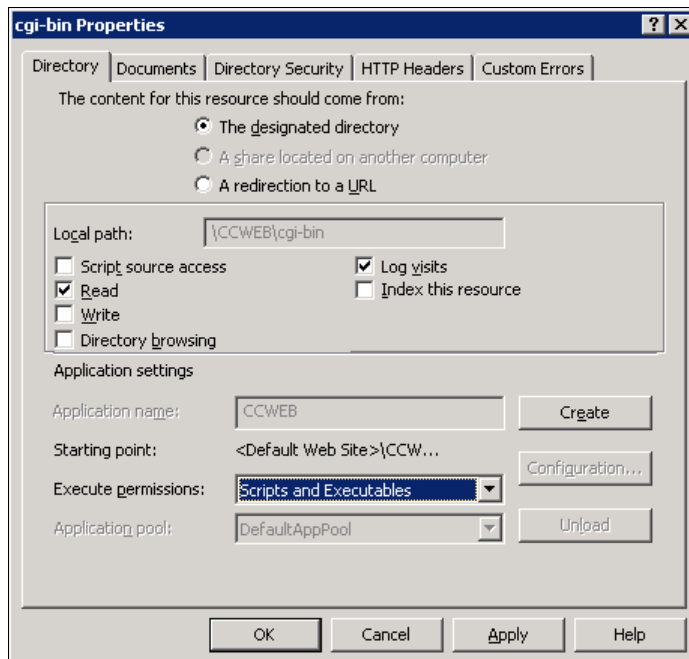
Step 10

Move to and right-click on **Internet Information Services** → ... (Local Computer) → **Web Sites** → **Default Web Site** → **CCWEB** → **cgi-bin** and select **Properties**.



Step 11

In the properties window select the tab **Directory**. There you select under **Execute permissions: Scripts and Executables**. Save all setting by leaving this window with **OK**.



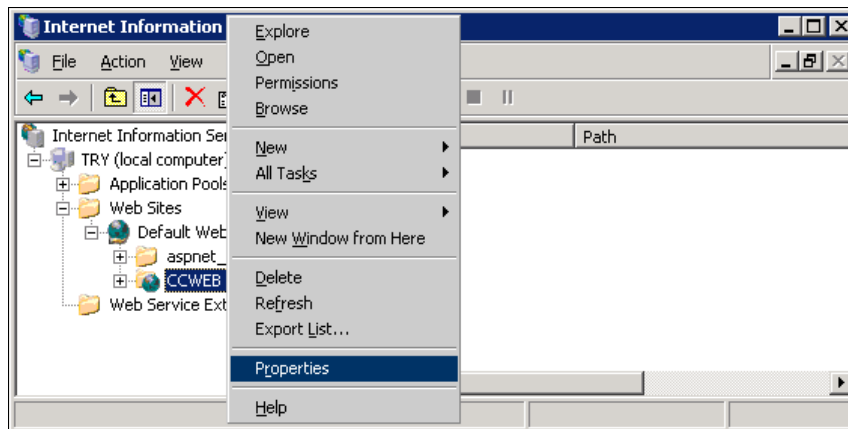
3.2.2 Setting up Authentication

Important: By default the IIS will grant access to hosted web sites with the anonymous/guest account. Due to the lack of permissions, this account cannot be used to administrate CompanyCRYPT. Please use the administrators account or an account with sufficient permissions to fully access the CompanyCRYPT folder and additional rights to install/start/stop services.

It is highly recommended to activating this setting by which access to the CompanyCRYPT WebGUI is only granted after successful authentication.

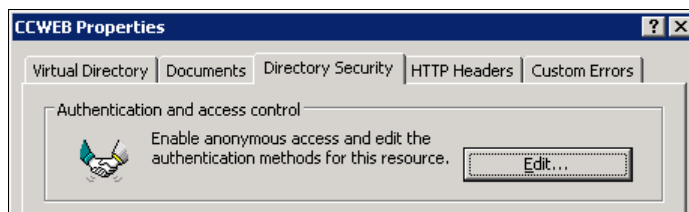
Step 1

Right-click on **Internet Information Services** → ... (Local Computer) → **Web Sites** → **Default Web Site** → **CCWEB** and select **Properties**.



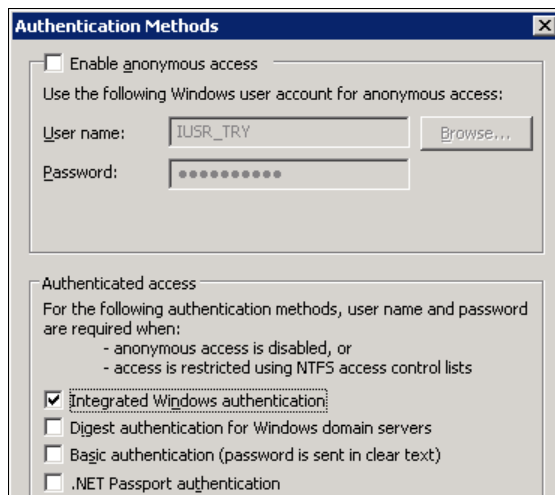
Step 2

In the properties window select the tab **Directory Security**. Click in the button **Edit...** in the section **Authentication and access control**.



Step 3

Deactivate the first check box **Enable anonymous access**. Instead **activate** the check box **Integrated Windows authentication**.



3.2.3 Setting up Access Control

The implementation of access control is based on the windows user management. It is recommended to set up a dedicated user group in the system that is afterwards configured to have access to the CompanyCRYPT WebGUI.

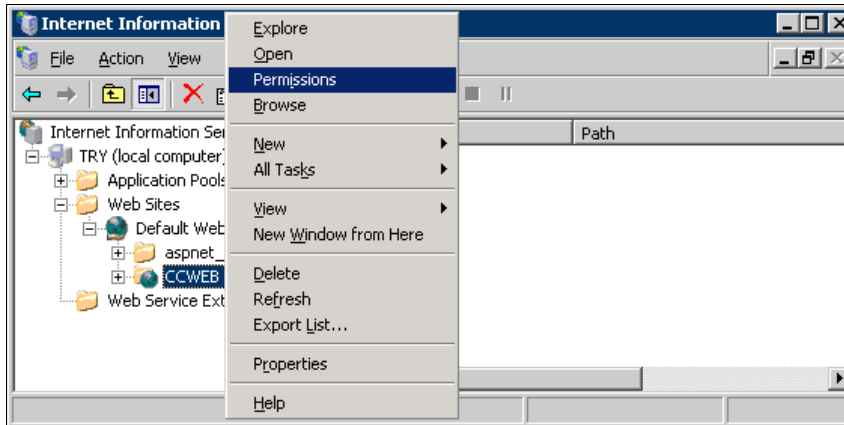
Step 1

Set up a new user group. Depending on the existing infrastructure it may either be a local or a domain group. For better recognisability name this group CompanyCRYPT-Administrators. Add all desired personal accounts to make them members of that group.



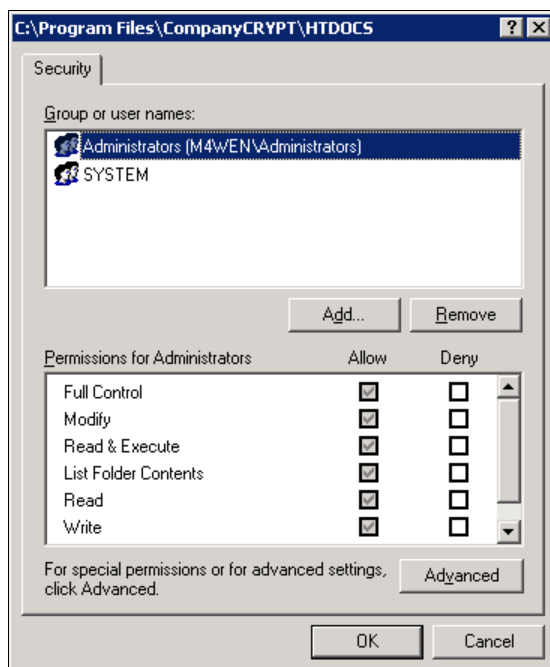
Step 2

Right-click on **Internet Information Services** → ... (Local Computer) → **Web Sites** → **Default Web Site** → **CCWEB** and select **Permissions**.



Step 3

Make sure that besides the **System** account (required) only accounts and groups are listed that are entitled to manage CompanyCRYPT. All other entries are to be removed. The remaining accounts should be configured to have **Full Control**. Save the settings by clicking on **OK**.



Important: All members of the group CompanyCRYPT-Administrators have to be also members of the main administrators group! This is required to ensure full access to the CompanyCRYPT installation folder and the right to set up and control services.

3.2.4 Activating SSL encryption (optional, recommended)

All data and information entered via the WebGUI can be protected during transmission from your browser to the server by means of SSL encryption. The ability of using SSL has to be activated in the IIS. This can be done at any given time.

Important: Activation of SSL in the IIS requires the import of a server-certificate, usually supplied in the form of a *.p12 file. This cannot be generated within the IIS. You may buy a web certificate from a trustcenter. Alternatively you can use your CompanyCRYPT installation to generate a suitable file. See the Configuration Guide in the chapter about Partner certificates on how to get such a file.

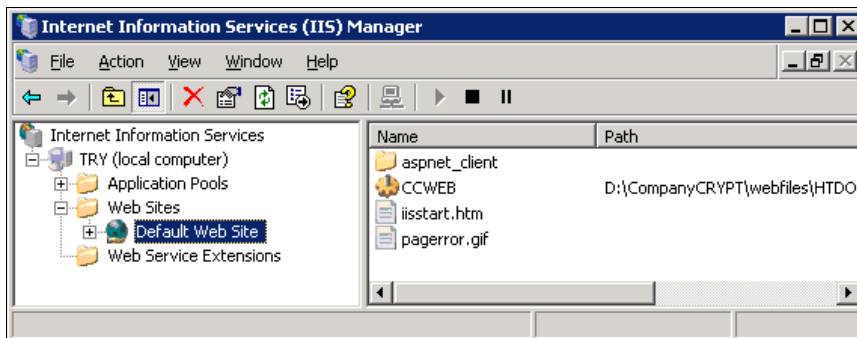


Note: Make sure that the name of the certificate owner exactly matches the FQDN (Fully Qualified Domain Name) of your server. Example: <http://msw.company.com/cc-web> → Name: **msw.company.com**

Step 1

Note: If there is already a server certificate integrated into your *Default Web Site* this step is obsolete.

Move to and right-click on **Internet Information Services → ... (Local Computer) → Web Sites → Default Web Site** and select **Properties**.

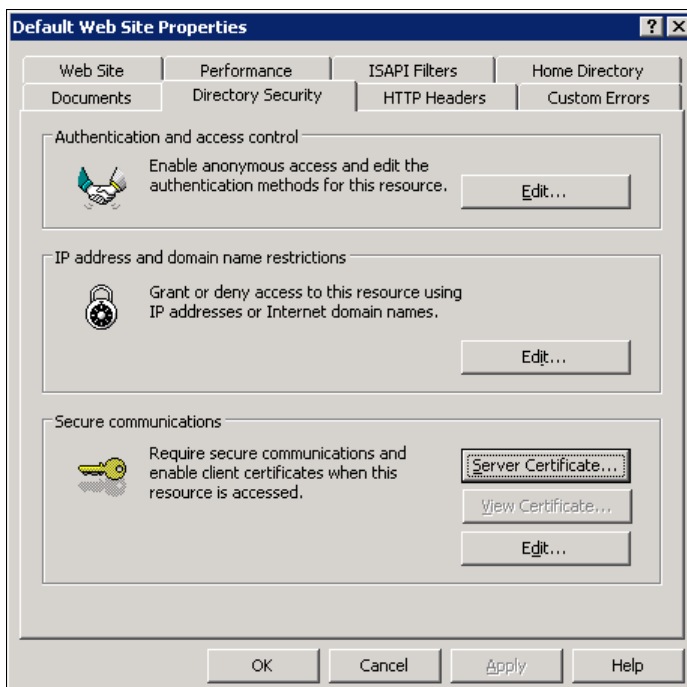


Step 2

Note: If there is already a server certificate integrated into your *Default Web Site* this step is obsolete.

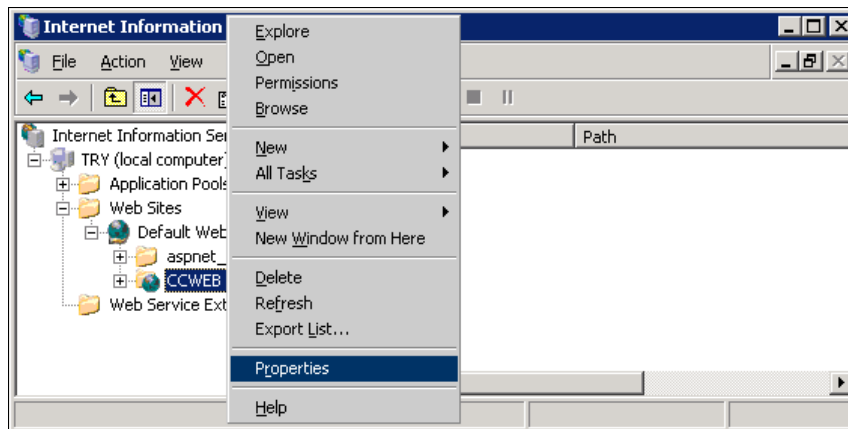
In the properties window select the tab **Directory Security**. Click in the button **Server Certificate** in the section **Secure Communication** in order to import the certificate.

Now follow all necessary steps to import the server certificate.



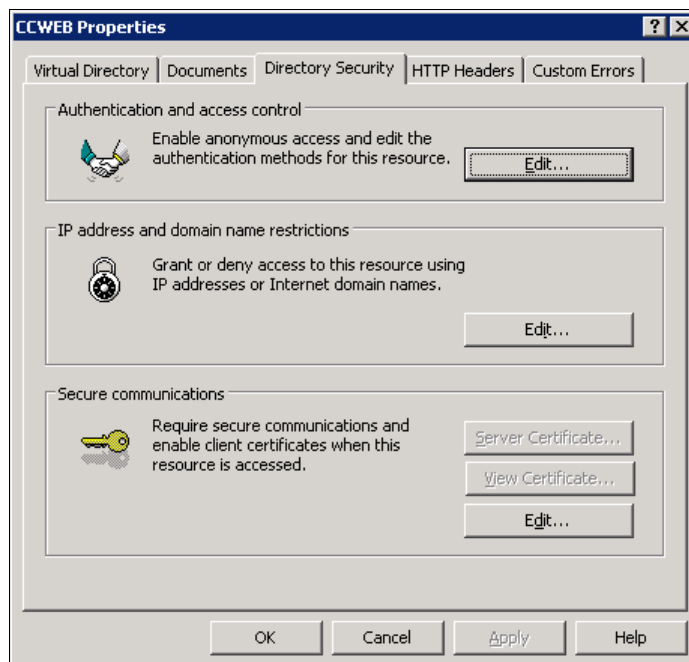
Step 3

Right-click on **Internet Information Services → ... (Local Computer) → Web Sites → Default Web Site → CCWEB** and select **Properties**.



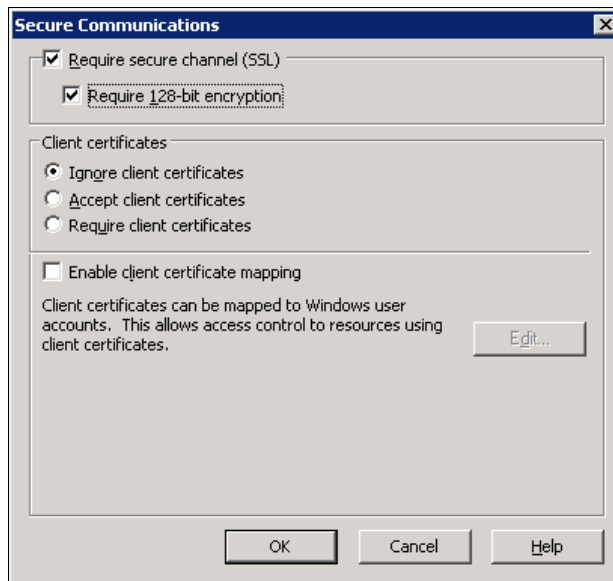
Step 4

In the properties window select the tab **Directory Security**. Click in the button **Edit...** in the section **Secure communications**.



Step 5

Activate the first check-box **Require secure channel (SSL)** and the following **Require 128-bit encryption**. Save all settings by leaving this window with **OK**.



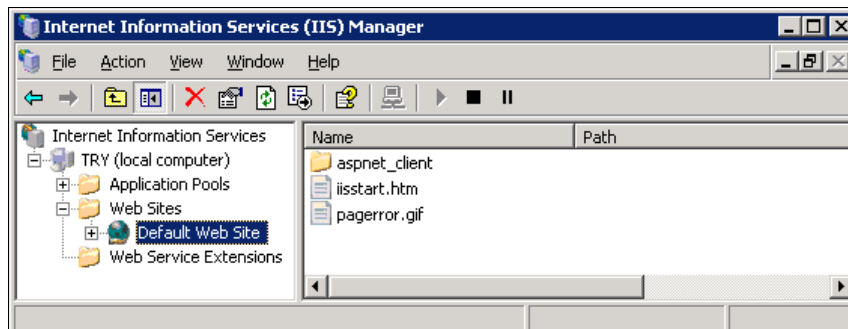
3.2.5 Setting up the URL for Certificate Revocation List – CRL

If a self-signed CA certificate is used within CompanyCRYPT for creating and signing of new certificates, then a certificate revocation list will be created automatically by CompanyCRYPT. This CRL will typically be provided via a HTTP link.

The address of the CRL consists of the domain (of the hostname) and the selected directory. Example: mail.host.com/CRL

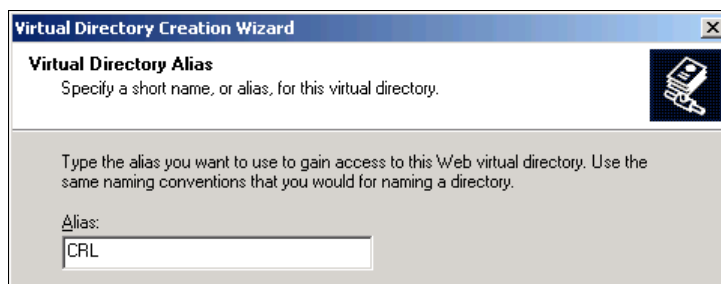
Step 1

Begin with **Start → All Programs → Administrative Tools** and start the **Internet Information Services (IIS) Manager**. Move to **Internet Information Services → ... (Local Computer) → Web Sites** and select **Default Web Site**.



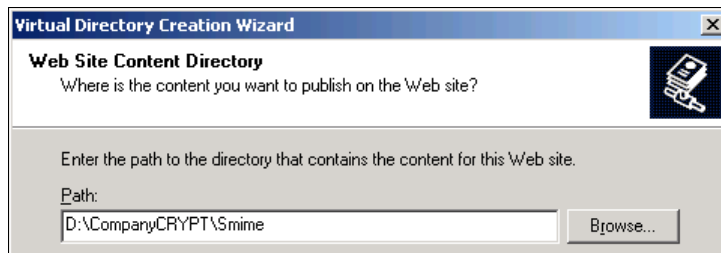
Step 2

Right-click on **Default Web Site** and select **New → Virtual Directory**. Enter **CRL** as an alias or choose an individual name.



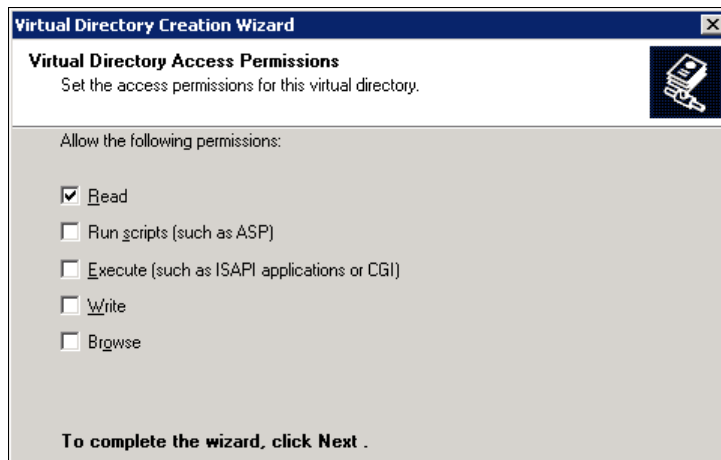
Step 3

Enter the following path according to your installation: **<CC-Install directory>\smime**



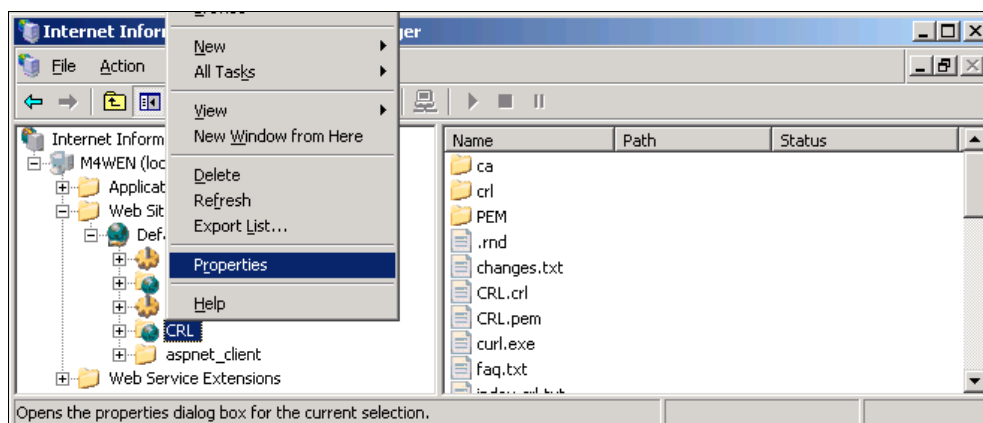
Step 4

Under permissions only mark **Read**.



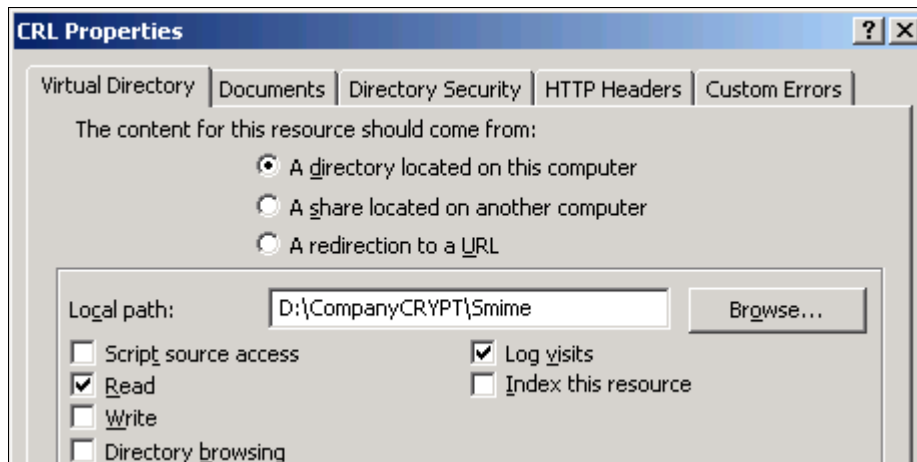
Step 5

Right-click on **Internet Information Services** → ... (Local Computer) → **Web Sites** → **Default Web Site** → **CRL** and select **Properties**.



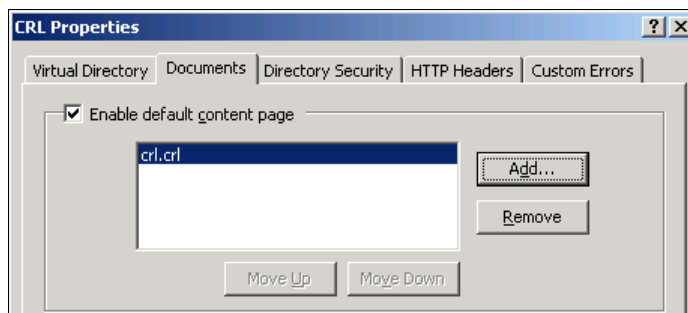
Step 6

In the properties window select the tab **Virtual Directory**. Now mark the permission **Read**, deactivate **Index this resource** and select under **Execute permissions: None**.



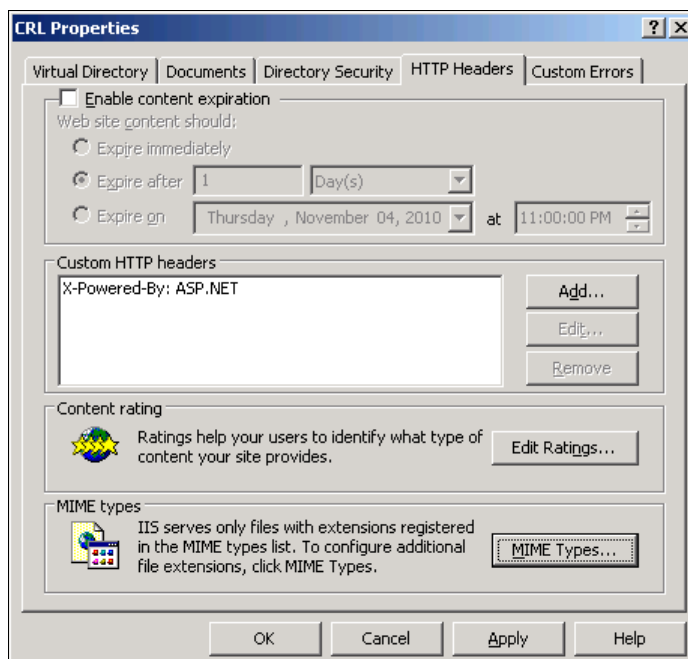
Step 7

Continue in the properties window and move to **Documents**. Activate the option **Enable default content page**. Remove all entries from the list and add the file name **crl.crl**.



Step 8

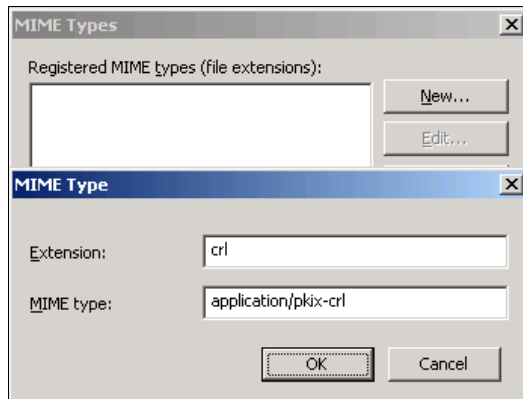
Move to the tab **HTTP Headers** and select the button **MIME Types**.



Step 9

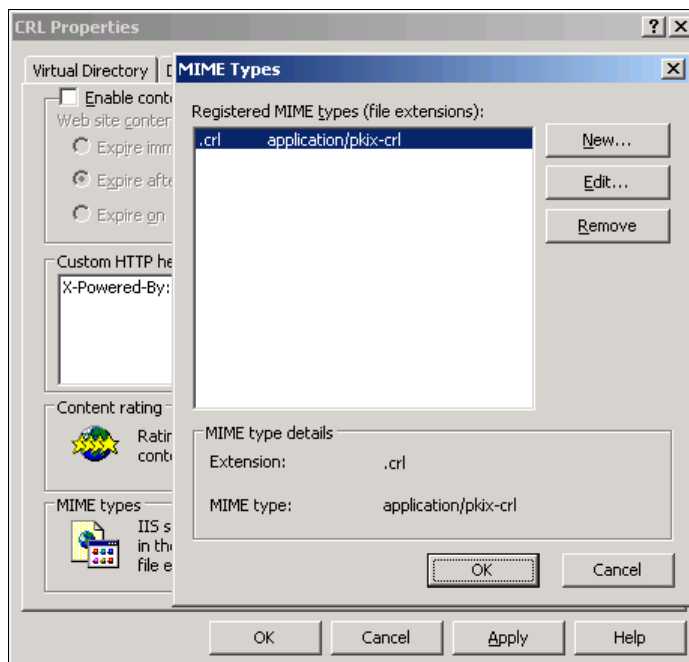


In the window **MIME Types** add an entry with **New**. Type **CRL** into the field Extension and **application/pkix-crl** into the field MIME type. Save this settings with **OK**.



Step 10

Close the window MIME Types with **OK** and save all setting by leaving the window with **OK**.



Note: All internal certificates should contain the link to your CRL. This will provide the information about the CRL to your partners for automated queries. Full URL syntax is required. Example: <http://mail.host.com/CRL>

Important: Note that to access the Certificate Revocation List via HTTP from the Internet your firewall rules have to be modified as well.

3.3 Installing the WebGUI under Microsoft® Windows Server 2008 / 2008 R2

The following pages will describe the integration into a Microsoft® Internet Information Service (IIS) 7.0 under Windows Server 2008 R2. Upon integration into an older version of the IIS (or MS-Windows) the name of some paths and menu items may differ from the documented information hereafter.



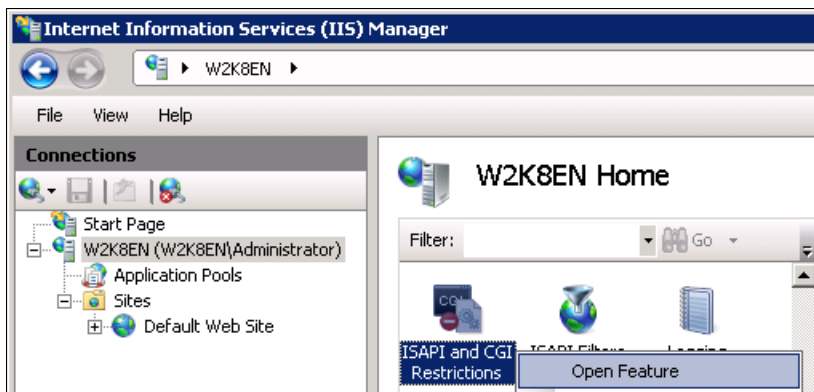
Important: For the configuration of the WebGUI the **Role „Web Server (IIS)“** and the **Role Services „CGI“** and **„URL Authorization“** must be installed on the server. Within the Server Manager you can install the needed components.

3.3.1 Setting up the CC-WebGUI as a Virtual Directory

The implementation as a Virtual Directory is highly recommended. It means that when accessing the CompanyCRYPT-WebGUI, the address consists of the domain (of the hostname) and the selected directory for CompanyCRYPT. Example: mail.host.com/CCWEB

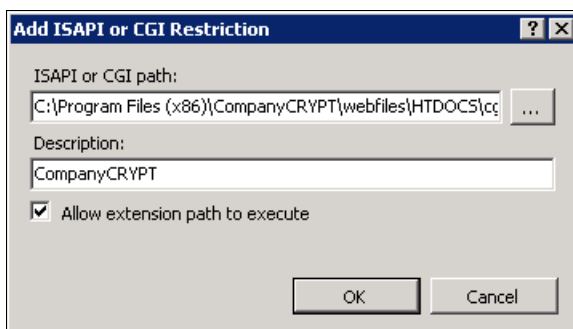
Step 1

Begin with **Start → Administrative Tools** and start the **Internet Information Services (IIS) Manager**. Move to and right-click on **Internet Information Services (IIS) Manager → ... (Local Computer) → (Features View) ISAPI and CGI Restrictions** and select **Open Feature**.



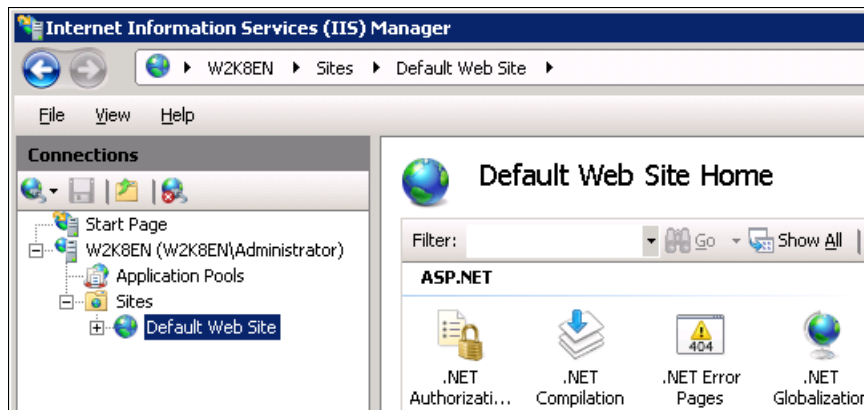
Step 2

Now click on the Action **Add** and add to the **ISAPI or CGI path**: **<CompanyCRYPT-Install directory>\webfiles\HTDOCS\cgi-bin\index.exe**. Enter **CompanyCRYPT** into the field **Description**. Finally activate the field **Allow extension path to execute** and save with **OK**.



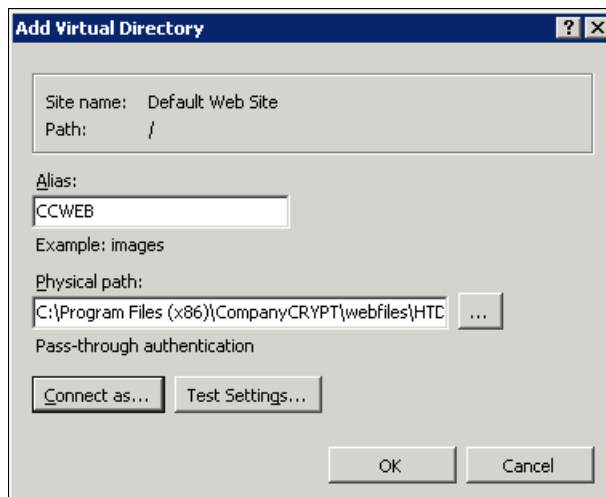
Step 3

Move to **Internet Information Services (IIS) Manager → ... (Local Computer) → Sites** and select **Default Web Site**.



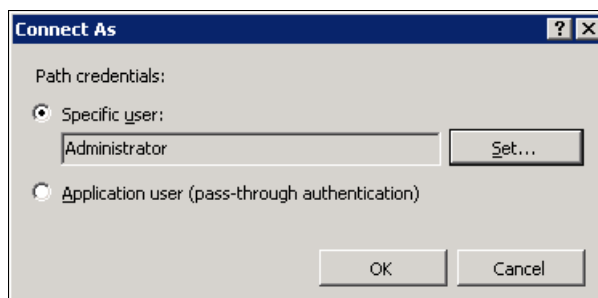
Step 4

Right-click on **Default Web Site** and select **Add Virtual Directory**. Enter **CCWEB** as an alias or choose an individual name. Enter the Physical path according to your installation: **<CC-Install directory>\Webfiles\HTDOCS**. Click on **Connect as**.



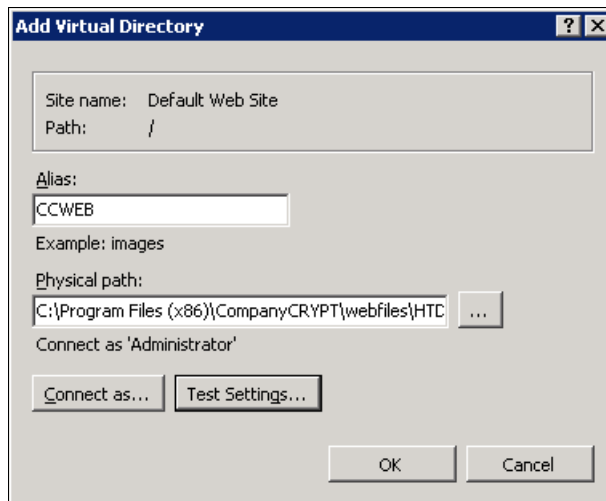
Step 5

Select **Specific user** and click the button **Set**. Enter the login credentials for the local **administrator** account and save the settings with **Ok**.



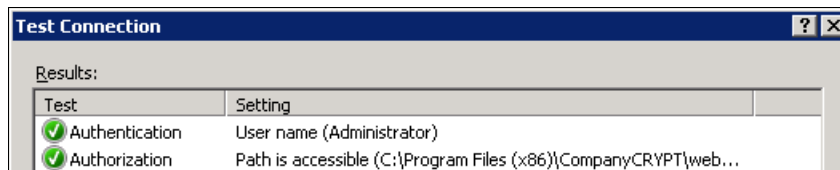
Step 6

Click on the button **Test Settings**.



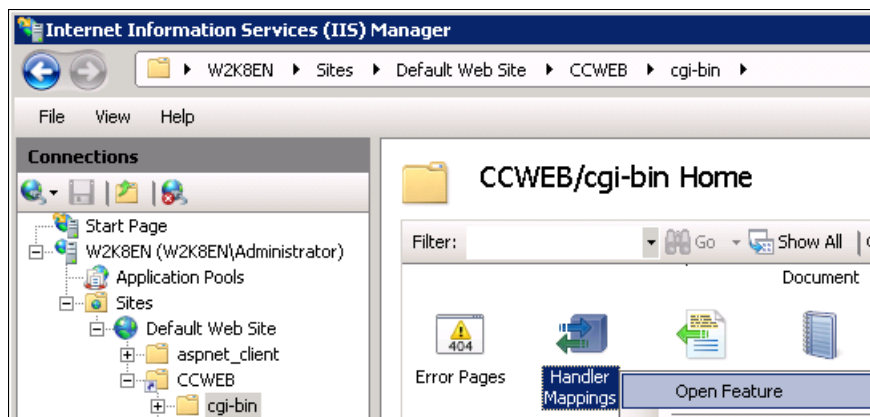
Step 7

Please check the login credentials of the local administrator account if the test results are not successful. If all settings entered correctly close the window **Add virtual Directory** with **OK**.



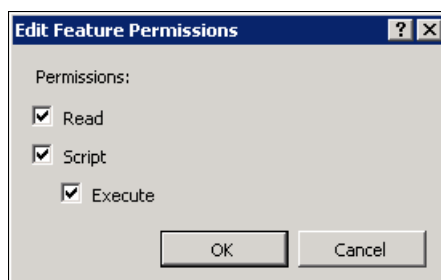
Step 8

Move to and right-click on **Internet Information Services (IIS) Manager** → ... (Local Computer) → Sites → Default Web Site → **CCWEB** → **cgi-bin** → **Handler Mappings** and select **Open Feature**.



Step 9

Now click on the Action **Edit Feature Permissions**. Finally activate **Execute** and save with **OK**.





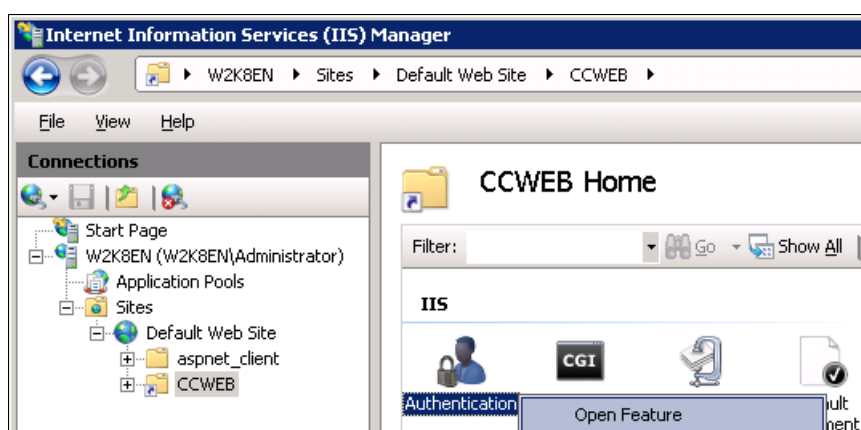
3.3.2 Setting up Authentication

Important: By default the IIS will grant access to hosted web sites with the anonymous/guest account. Due to the lack of permissions, this account cannot be used to administrate CompanyCRYPT. Please use the administrators account or an account with sufficient permissions to fully access the CompanyCRYPT folder and additional rights to install/start/stop services.

It is highly recommended to activating this setting by which access to the CompanyCRYPT WebGUI is only granted after successful authentication.

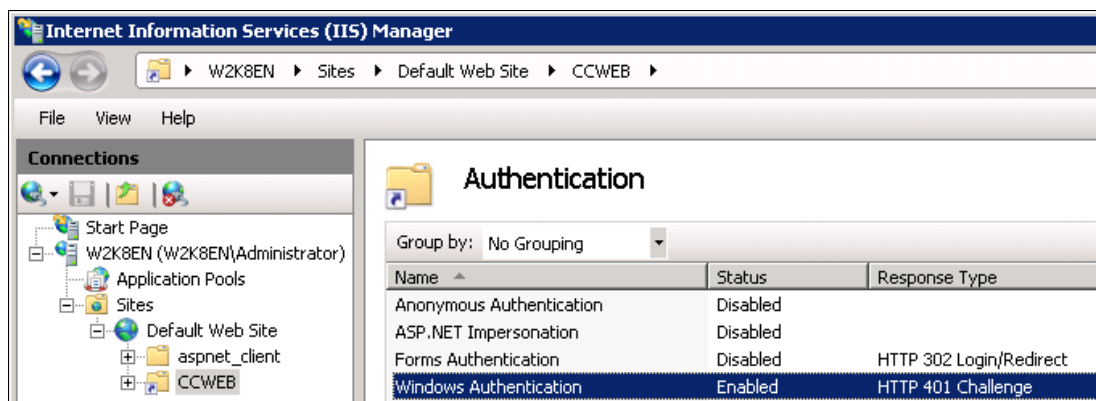
Step 1

Move to and right-click on **Internet Information Services (IIS) Manager** → ... (Local Computer) → **Sites** → **Default Web Site** → **CCWEB** → **Authentication** and select **Open Feature**.



Step 2

Disable the **Anonymous Authentication**. Instead **activate the Windows Authentication**.



3.3.3 Setting up Access Control

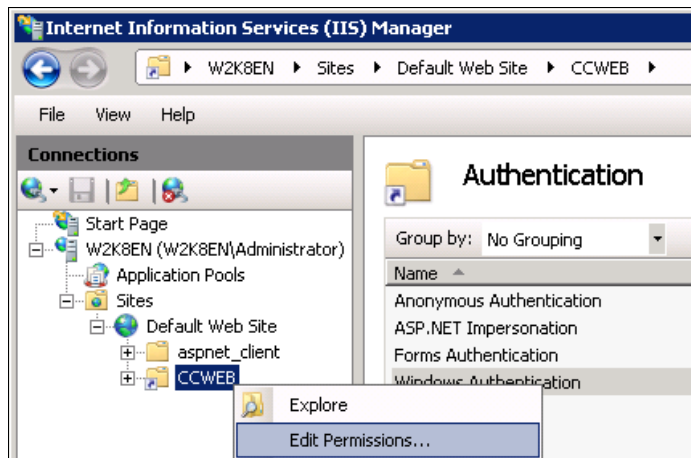
The implementation of access control is based on the windows user management. It is recommended to set up a dedicated user group in the system that is afterwards configured to have access to the CompanyCRYPT WebGUI.

Step 1

Set up a new user group. Depending on the existing infrastructure it may either be a local or a domain group. For better recognisability name this group CompanyCRYPT-Administrators. Add all desired personal accounts to make them members of that group.

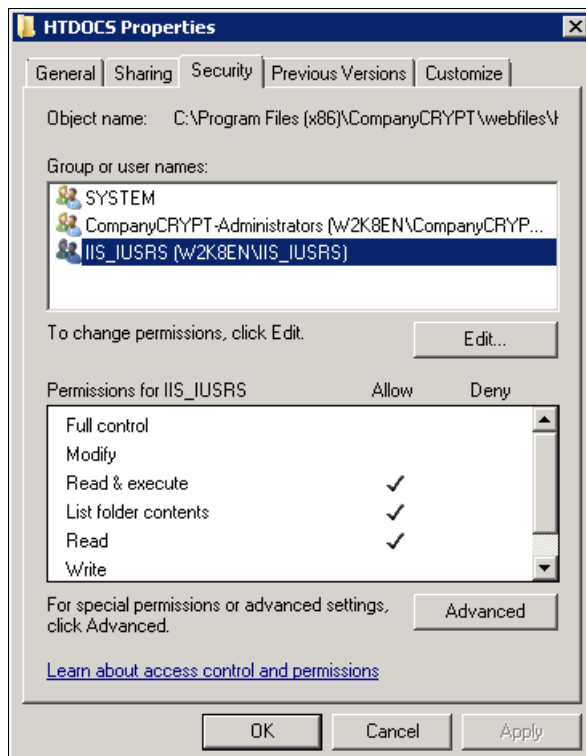
Step 2

Move to and right-click on **Internet Information Services (IIS) Manager** → ... (Local Computer) → **Sites** → **Default Web Site** → **CCWEB** and select **Edit Permissions**.



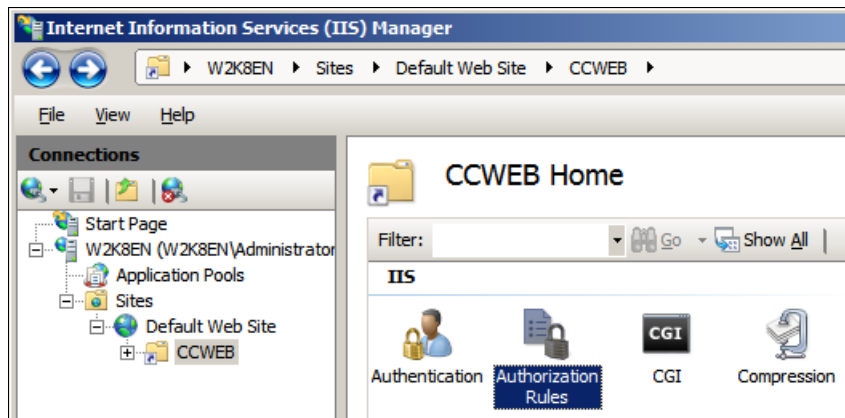
Step 3

Make sure that besides the **System** account (required) only accounts and groups are listed that are entitled to manage CompanyCRYPT. All other entries are to be removed. This accounts should be configured to have **Full Control**. Add the account **IIS_IUSRS** with the following permissions: 'Read & execute', 'List folder contents' and 'Read'. Save the settings by clicking on **OK**.



Step 4

Move to and right-click on **Internet Information Services (IIS) Manager** → ... (Local Computer) → **Sites** → **Default Web Site** → **CCWEB** → **Authorization Rules** and select **Open Feature**.



Step 5

Remove all Rules from the list and click on the Action **Add Allow Rule**. Select **Specified roles or user groups** and enter the group **CompanyCRYPT-Administrators**. Save with **OK**.



3.3.4 Activating SSL encryption (optional, recommended)

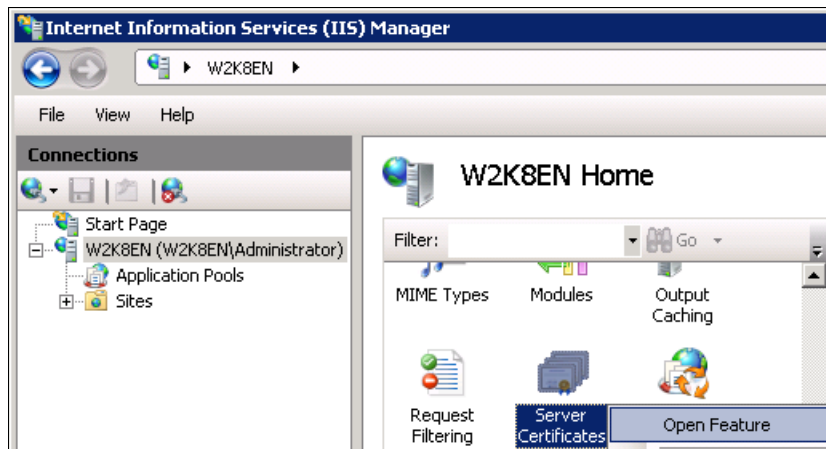
All data and information entered via the WebGUI can be protected during transmission from your browser to the server by means of SSL encryption. The ability of using SSL has to be activated in the IIS. This can be done at any given time.

Note: Activation of SSL in the IIS requires the import of a server-certificate, usually supplied in the form of a *.p12 file. This can be generated within the IIS.

Note: If there is already a server certificate integrated into your *Default Web Site* this step is obsolete.

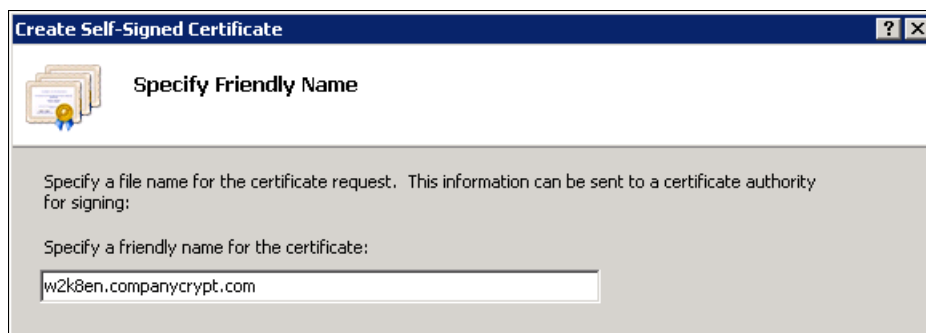
Step 1

Move to and right-click on **Internet Information Services (IIS) Manager** → ... **(Local Computer)** → **Server Certificates** and select **Open Feature**.



Step 2

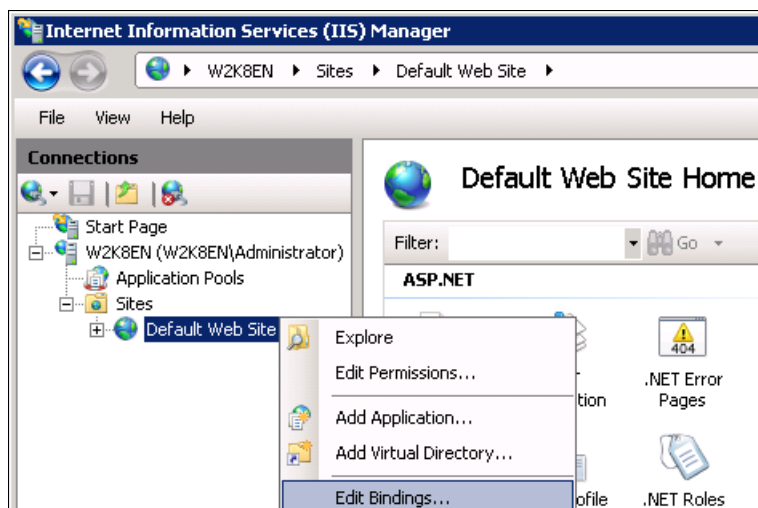
Now click on the Action **Create Self-Signed Certificate**. Add the Fully Qualified Domain Name of the server to the field **Specify a friendly name for the certificate**. Save with **OK**.



Important: Make sure that the name of the certificate owner exactly matches the FQDN (Fully Qualified Domain Name) of your server. Example: <http://msw.company.com/ccweb> → Name: **msw.company.com**

Step 3

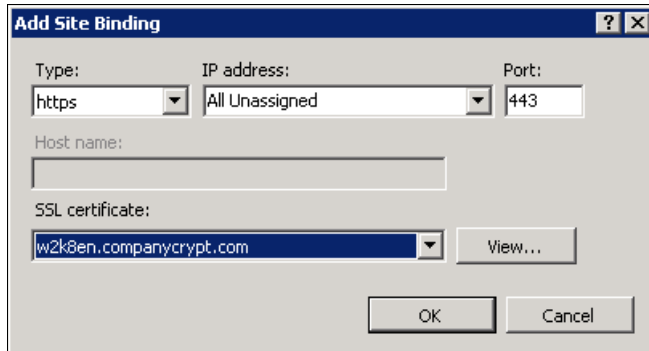
Move to and right-click on **Internet Information Services (IIS) Manager** → ... (Local Computer) → **Sites** → **Default Web Site** and select **Edit Bindings**.





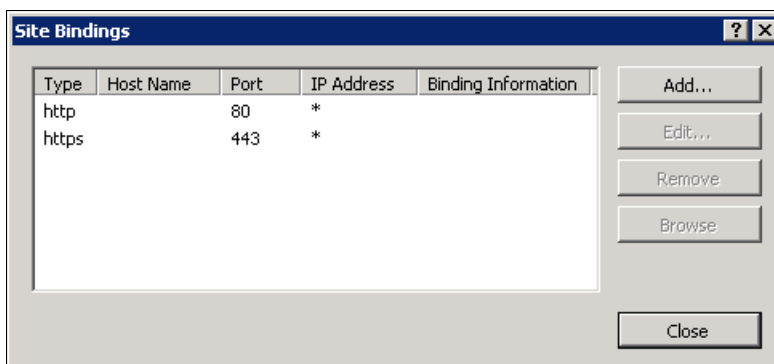
Step 4

In the window Site Bindings click the button **Add**. Select **https** in the field **Type** and in the field **SSL certificate** choose the entry which matches the local **server name**. Save all setting by leaving this window with **OK**.



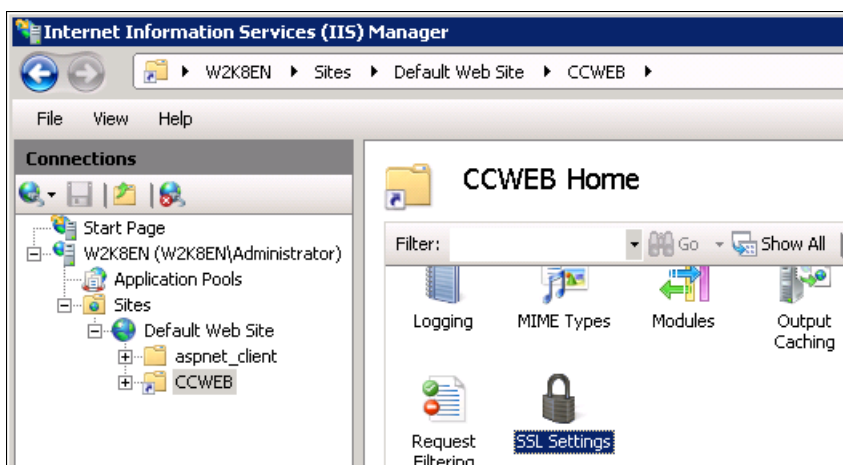
Step 5

The windows Site Bindings will show the entry for https. **Close** this window.



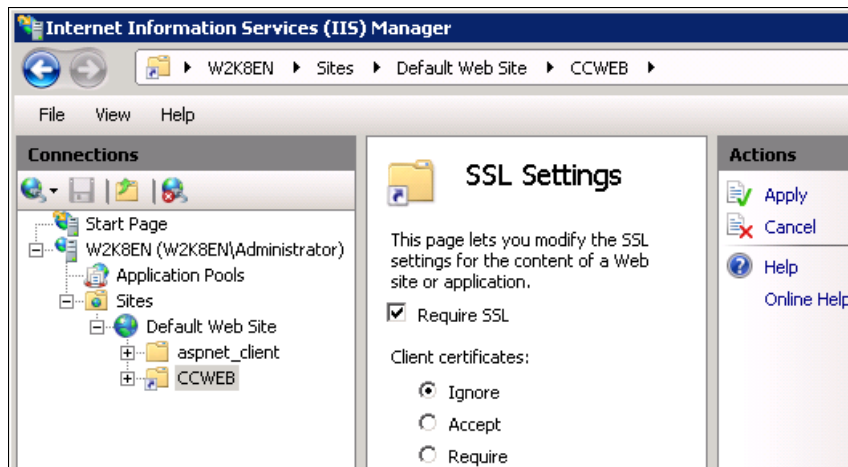
Step 6

Move to and right-click on **Internet Information Services (IIS) Manager** → ... (Local Computer) → Sites → Default Web Sites → **CCWEB** → **SSL settings** and select **Open Feature**.



Step 7

Activate the option **Require SSL**. The Client certificates settings should be set to **Ignore**. Save the settings with **Apply**.



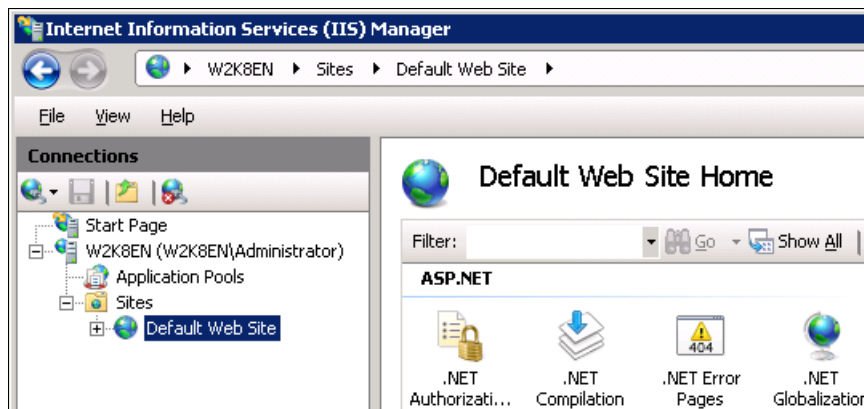
3.3.5 Setting up the URL for Certificate Revocation List – CRL

If a self-signed CA certificate is used within CompanyCRYPT for creating and signing of new certificates, then a certificate revocation list will be created automatically by CompanyCRYPT. This CRL will typically be provided via a HTTP link.

The address of the CRL consists of the domain (of the hostname) and the selected directory. Example: mail.host.com/CRL

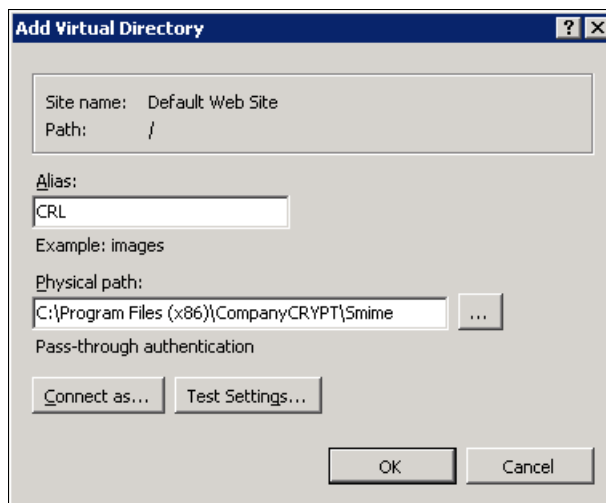
Step 1

Begin with **Start → Administrative Tools** and start the **Internet Information Services (IIS) Manager**. Move to **Internet Information Services (IIS) Manager → ... (Local Computer) → Sites** and select **Default Web Site**.



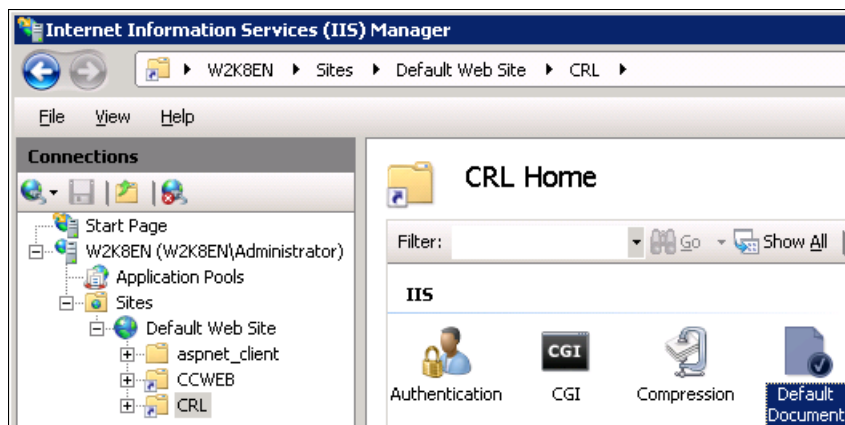
Step 2

Right-click on **Default Web Site** and select **Add Virtual Directory**. Enter **CRL** as an alias or choose an individual name. Enter the Physical path according to your installation: **<CC-Install directory>\smime** and save with **OK**.



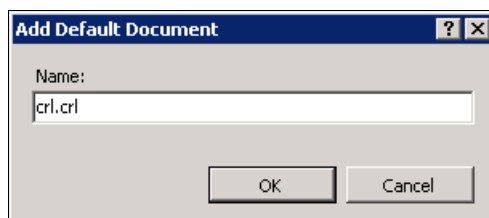
Step 3

Move to and right-click on **Internet Information Services (IIS) Manager** → ... (Local Computer) → Sites → Default Web Sites → CRL → **Default Document** and select **Open Feature**.



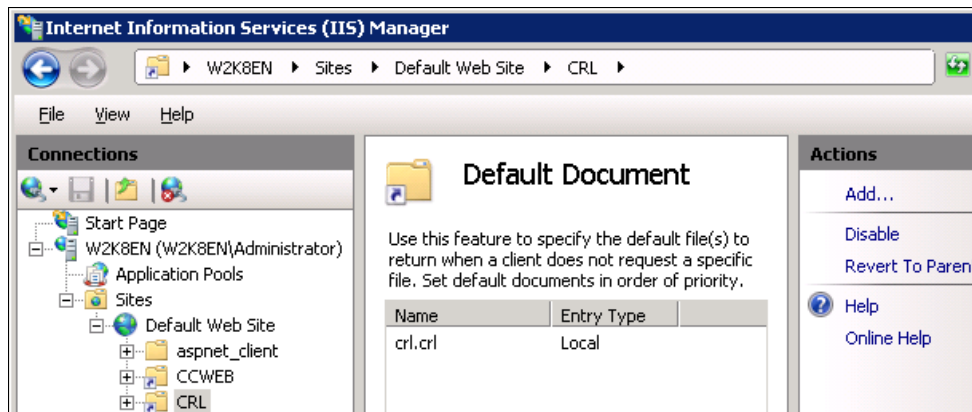
Step 4

Choose the Action **Add** and enter the name **crl.crl** as the Default Document. Save with **OK**.



Step 5

Remove all entries from the list except the file name **crl.crl**.



Note: All internal certificates should contain the link to your CRL. This will provide the information about the CRL to your partners for automated queries. Full URL syntax is required. Example: <http://mail.host.com/CRL>

Important: Note that to access the Certificate Revocation List via HTTP from the Internet your firewall rules have to be modified as well.

3.4 Installing the WebGUI under Microsoft® Windows Server 2012 / 2012 R2

The following pages will describe the integration into a Microsoft® Internet Information Service (IIS) 7.0 under Windows Server 2008 R2. Upon integration into an older version of the IIS (or MS-Windows) the name of some paths and menu items may differ from the documented information hereafter.

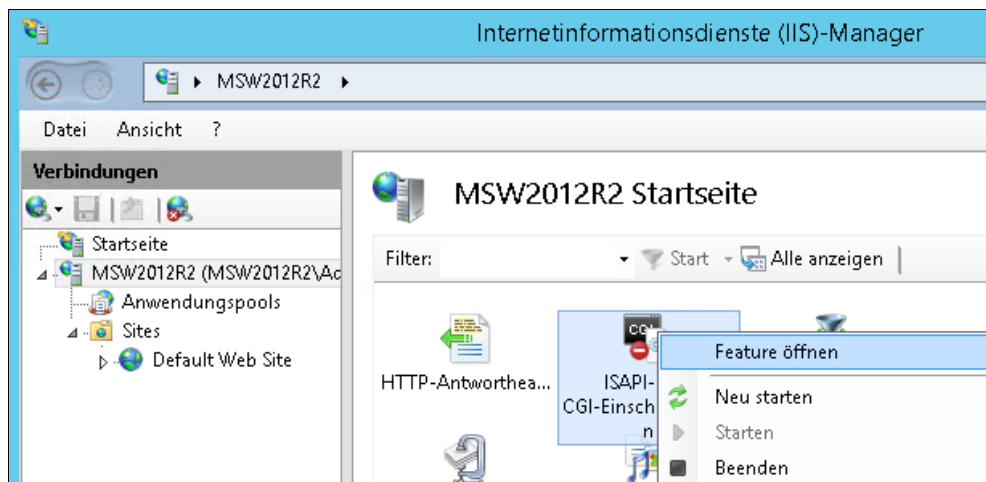
Important: For the configuration of the WebGUI the **Role „Web Server (IIS)“** and the **Role Services „CGI“** and **„URL Authorization“** must be installed on the server. Within the Server Manager you can install the needed components.

3.4.1 Setting up the CC-WebGUI as a Virtual Directory

The implementation as a Virtual Directory is highly recommended. It means that when accessing the CompanyCRYPT-WebGUI, the address consists of the domain (of the hostname) and the selected directory for CompanyCRYPT. Example: mail.host.com/CCWEB

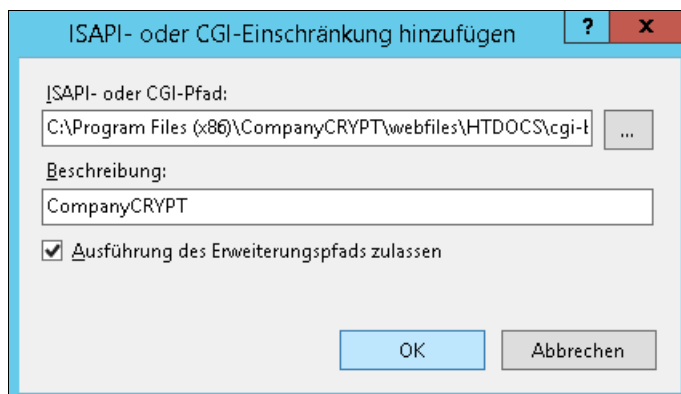
Step 1

Move to the **Desktop** and start the **Server Manager**. Click on **Tools → Internet Information Services (IIS) Manager**. Move to and right-click on **Internet Information Services (IIS) Manager → ... (Local Computer) → (Features View) ISAPI and CGI Restrictions** and select **Open Feature**.



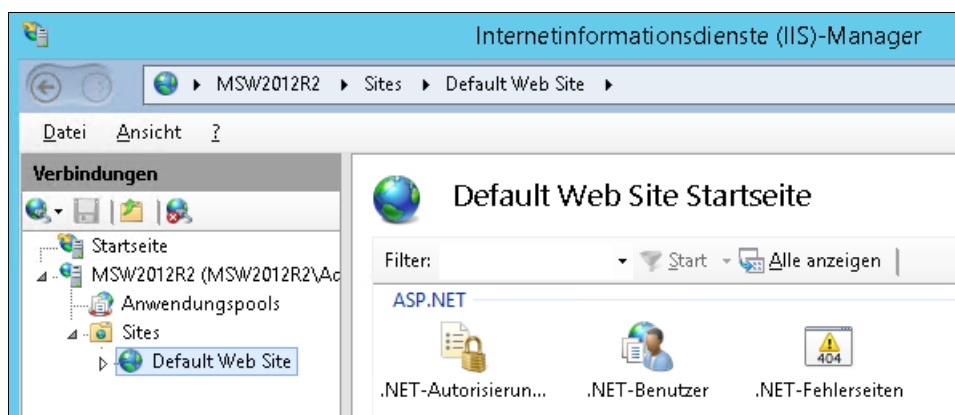
Step 2

Now click on the Action **Add** and add to the **ISAPI or CGI path**: **<CompanyCRYPT-Install directory>\webfiles\HTDOCS\cgi-bin\index.exe**. Enter **CompanyCRYPT** into the field **Description**. Finally activate the field **Allow extension path to execute** and save with **OK**.



Step 3

Move to **Internet Information Services (IIS) Manager** → ... **(Local Computer)** → **Sites** and select **Default Web Site**.



Step 4

Right-click on **Default Web Site** and select **Add Virtual Directory**. Enter **CCWEB** as an alias or choose an individual name. Enter the Physical path according to your installation: **<CC-Install directory>\Webfiles\HTDOCS**. Click on **Connect as**.



Virtuelles Verzeichnis hinzufügen

Sitename: Default Web Site
Pfad: /

Alias:
CCWEB

Beispiel: Bilder

Physischer Pfad:
C:\Program Files (x86)\CompanyCRYPT\webfiles\HTDO... ..

Pass-Through-Authentifizierung

Verbinden als... Einstellungen testen...

OK Abbrechen

Step 5

Select **Specific user** and click the button **Set**. Enter the login credentials for the local **administrator** account and save the settings with **Ok**.

Verbinden als

Pfadanmeldeinformationen:

☒ Bestimmter Benutzer:
Administrator Festlegen...

☐ Anwendungsbenutzer (Pass-Through-Authentifizierung)

OK Abbrechen

Step 6

Click on the button **Test Settings**.



Virtuelles Verzeichnis hinzufügen

Sitename: Default Web Site
Pfad: /

Alias:
CCWEB

Beispiel: Bilder

Physischer Pfad:
C:\Program Files (x86)\CompanyCRYPT\webfiles\HTDO... ..

Verbinden als "Administrator"

Verbinden als... Einstellungen testen...

OK Abbrechen

Step 7

Please check the login credentials of the local administrator account if the test results are not successful. If all settings entered correctly close the window **Add virtual Directory** with **OK**.

Verbindung testen

Ergebnisse:

Testen	Einstellung
✓ Authentifizierung	Benutzername (Administrator)
✓ Autorisierung	Auf den Pfad kann zugegriffen werden (C:\Program Files (x86)\CompanyCRYPT\web...

Step 8

Move to and right-click on **Internet Information Services (IIS) Manager** → ... (Local Computer) → **Sites** → **Default Web Site** → **CCWEB** → **cgi-bin** → **Handler Mappings** and select **Open Feature**.

Internetinformationsdienste (IIS)-Manager

MSW2012R2 > Sites > Default Web Site > CCWEB > cgi-bin

Verbindungen

- Startseite
- MSW2012R2 (MSW2012R2\Administrator)
- Anwendungspools
- Sites
 - Default Web Site
 - aspnet_client
 - CCWEB
 - cgi-bin
 - img
 - MIMESweeper for SMTP

CCWEB/cgi-bin Startseite

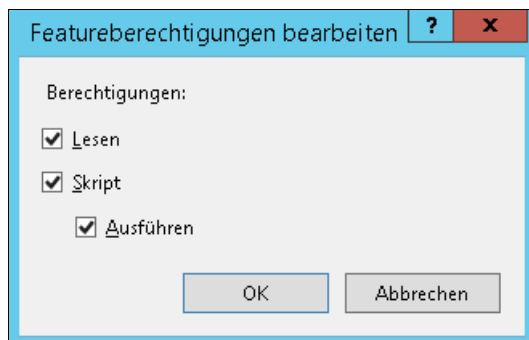
Filter: Start Alle anzeigen

Handlerzuordnun... HTTP-Antworthea... Komprimierung

MIME-Typ Module Protokollierung

Step 9

Now click on the Action **Edit Feature Permissions**. Finally activate **Execute** and save with **OK**.



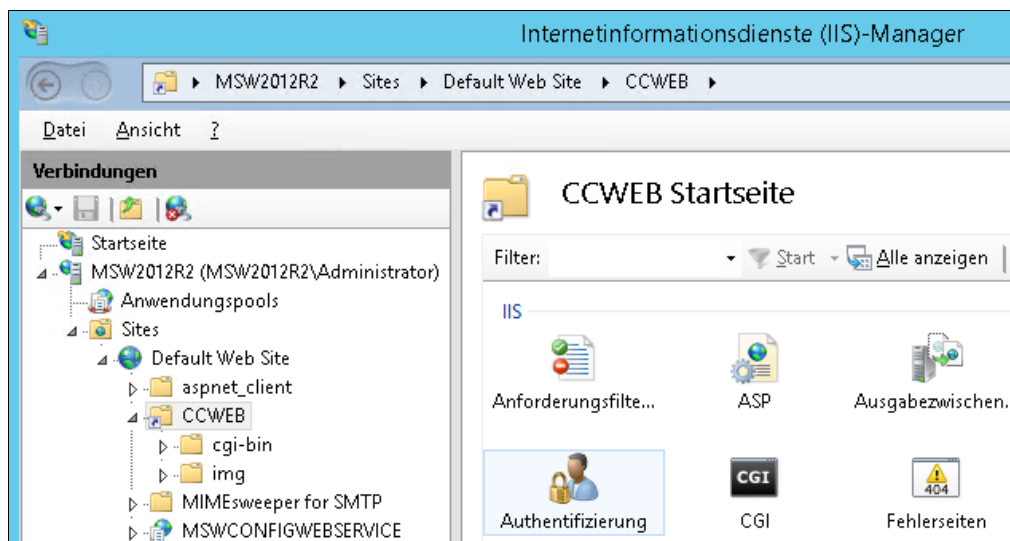
3.4.2 Setting up Authentication

Important: By default the IIS will grant access to hosted web sites with the anonymous/guest account. For security reasons, this access should be prevented and set up only to authorized persons.

It is highly recommended to activating this setting by which access to the CompanyCRYPT WebGUI is only granted after successful authentication.

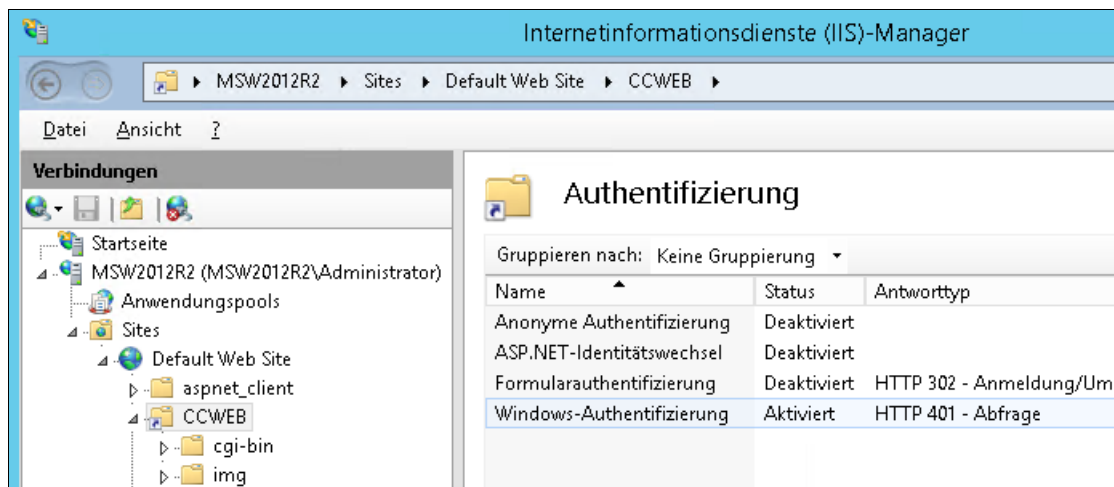
Step 1

Move to and right-click on **Internet Information Services (IIS) Manager** → ... (Local Computer) → **Sites** → **Default Web Site** → **CCWEB** → **Authentication** and select **Open Feature**.



Step 2

Disable the **Anonymous Authentication**. Instead **activate** the **Windows Authentication**.



3.4.3 Setting up Access Control

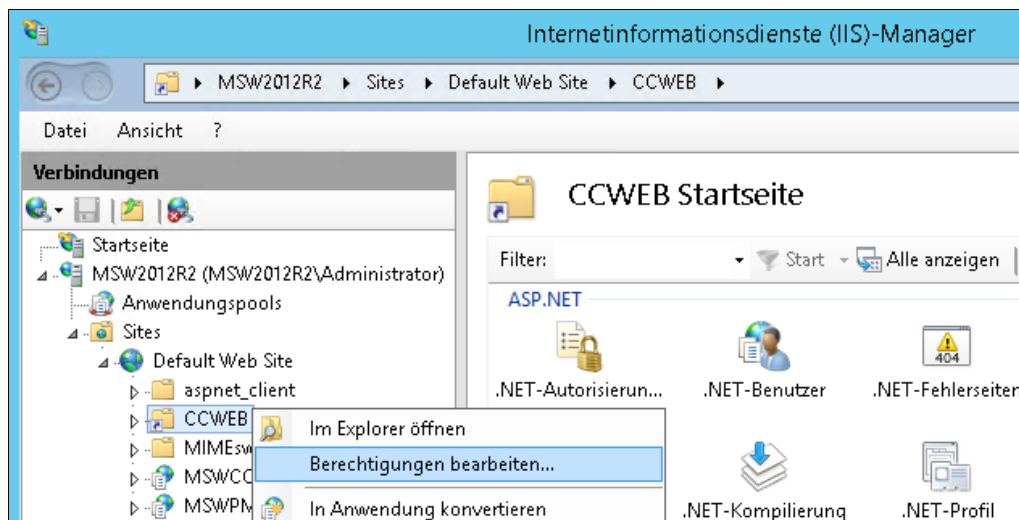
The implementation of access control is based on the windows user management. It is recommended to set up a dedicated user group in the system that is afterwards configured to have access to the CompanyCRYPT WebGUI.

Step 1

Set up a new user group. Depending on the existing infrastructure it may either be a local or a domain group. For better recognisability name this group **CompanyCRYPT-Administrators**. Add all desired personal accounts to make them members of that group.

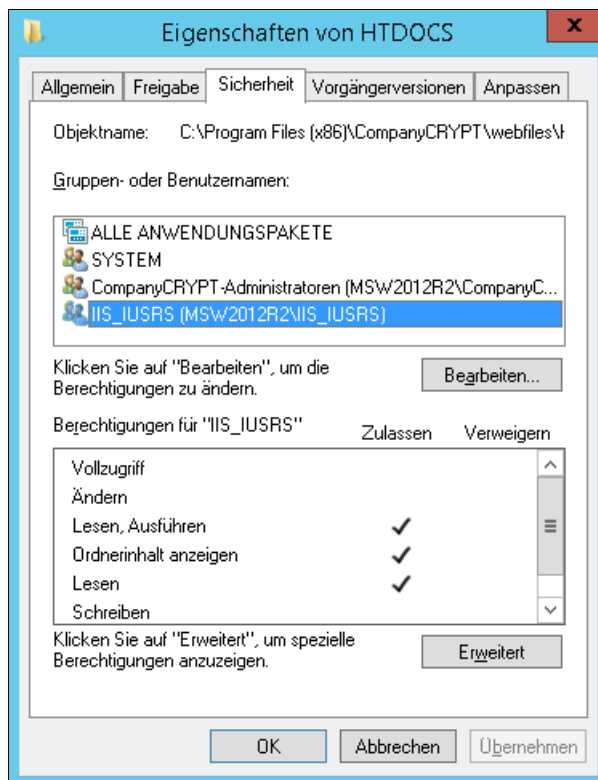
Step 2

Move to and right-click on **Internet Information Services (IIS) Manager** → ... (Local Computer) → **Sites** → **Default Web Site** → **CCWEB** and select **Edit Permissions**.



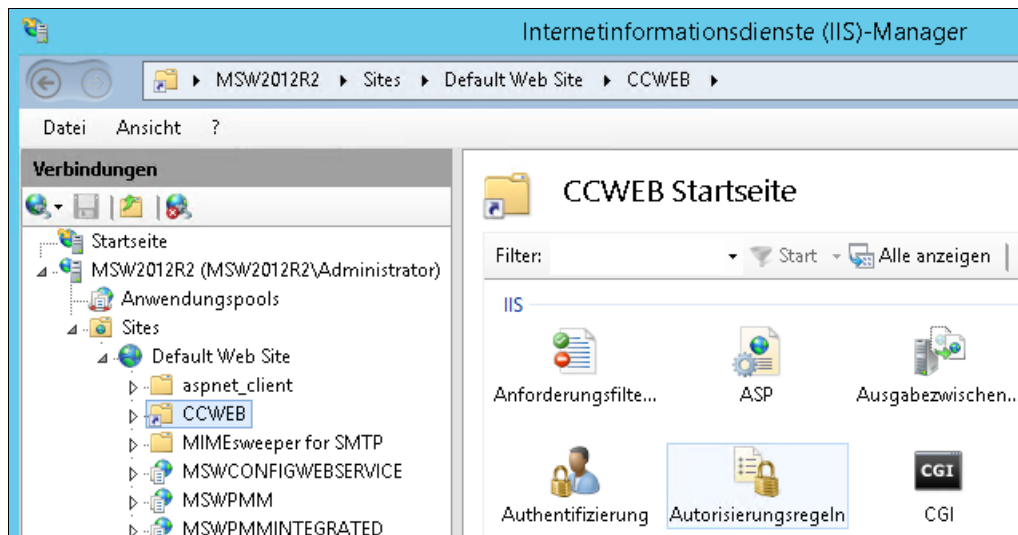
Step 3

Make sure that besides the **System** account (required) only accounts and groups are listed that are entitled to manage CompanyCRYPT. All other entries are to be removed. This accounts should be configured to have **Full Control**. Add the accounts **IIS_IUSRS** and **ALL APPLICATION PACKAGES** with the following permissions: 'Read & execute', 'List folder contents' and 'Read'. Save the settings by clicking on **OK**.



Step 4

Move to and right-click on **Internet Information Services (IIS) Manager** → ... (Local Computer) → **Sites** → **Default Web Site** → **CCWEB** → **Authorization Rules** and select **Open Feature**.



Step 5

Remove all Rules from the list and click on the Action **Add Allow Rule**. Select **Specified roles or user groups** and enter the group **CompanyCRYPT-Administrators**. Save with **OK**.



Autorisierungszulassungsregel hinzufügen

Zugriff auf diesen Webinhalt zulassen für:

☐ Alle Benutzer

☐ Alle anonymen Benutzer

☒ Bestimmte Rollen oder Benutzergruppen:

CompanyCRYPT-Administratoren

Beispiel: Administratoren

☐ Bestimmte Benutzer:

Beispiel: Benutzer1, Benutzer2

☐ Diese Regel auf bestimmte Verben anwenden:

Beispiel: GET, POST

OK Abbrechen

3.4.4 Activating SSL encryption (optional, recommended)

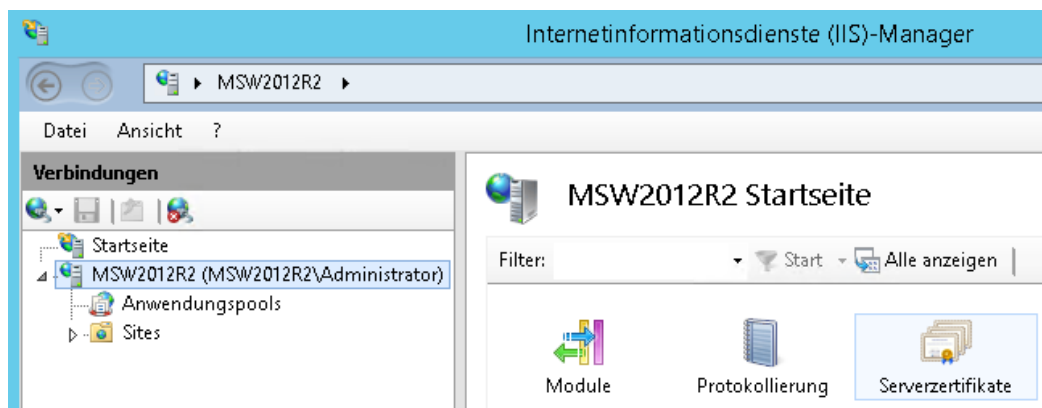
All data and information entered via the WebGUI can be protected during transmission from your browser to the server by means of SSL encryption. The ability of using SSL has to be activated in the IIS. This can be done at any given time.

Note: Activation of SSL in the IIS requires the import of a server-certificate, usually supplied in the form of a *.p12 file. This can be generated within the IIS.

Note: If there is already a server certificate integrated into your *Default Web Site* this step is obsolete.

Step 1

Move to and right-click on **Internet Information Services (IIS) Manager** → ... (Local Computer) → **Server Certificates** and select **Open Feature**.



Step 2

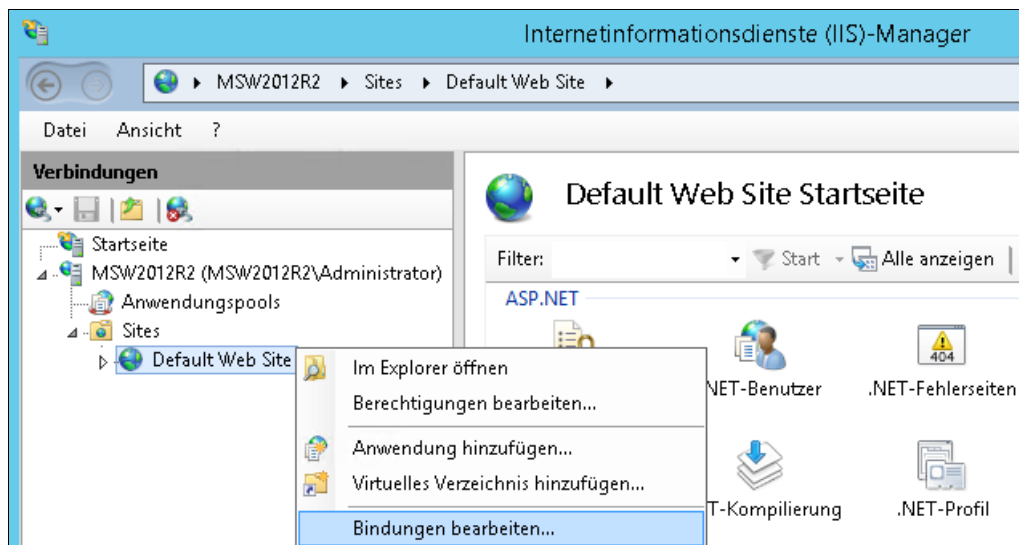


Now click on the Action **Create Self-Signed Certificate**. Add the Fully Qualified Domain Name of the server to the field **Specify a friendly name for the certificate**. Save with **OK**.

Important: Make sure that the name of the certificate owner exactly matches the FQDN (Fully Qualified Domain Name) of your server. Example: <http://msw.company.com/ccweb> → Name: **msw.company.com**

Step 3

Move to and right-click on **Internet Information Services (IIS) Manager** → ... (Local Computer) → **Sites** → **Default Web Site** and select **Edit Bindings**.



Step 4

In the window **Site Bindings** click the button **Add**. Select **https** in the field **Type** and in the field **SSL certificate** choose the entry which matches the local **server name**. Save all setting by leaving this window with **OK**.

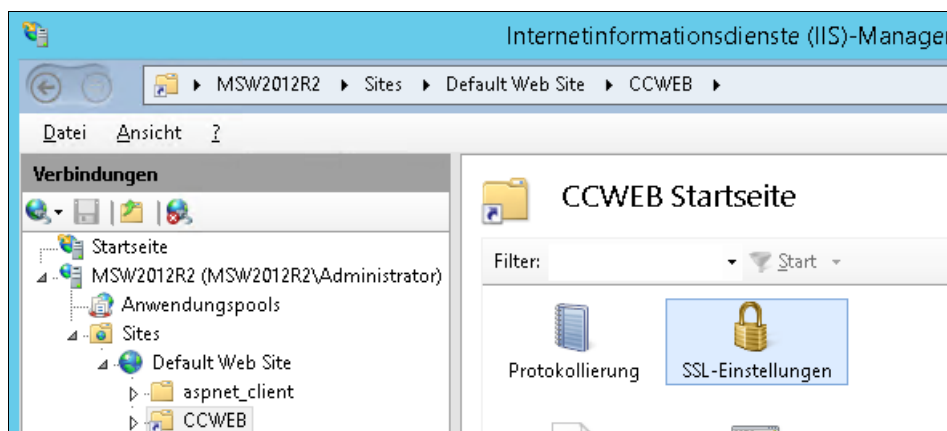


Step 5

The windows Site Bindings will show the entry for https. **Close** this window.

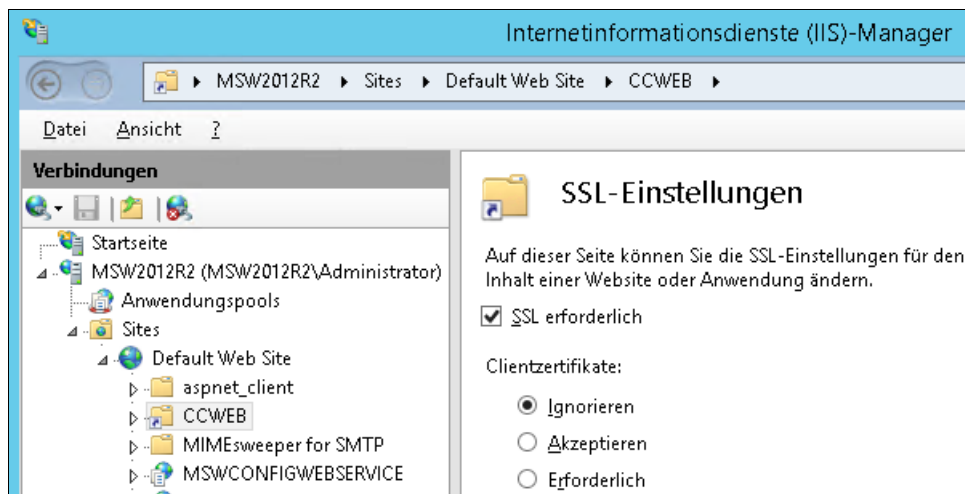
Step 6

Move to and right-click on **Internet Information Services (IIS) Manager** → ... (Local Computer) → **Sites** → **Default Web Sites** → **CCWEB** → **SSL settings** and select **Open Feature**.



Step 7

Activate the option **Require SSL**. The Client certificates settings should be set to **Ignore**. Save the settings with **Apply**.



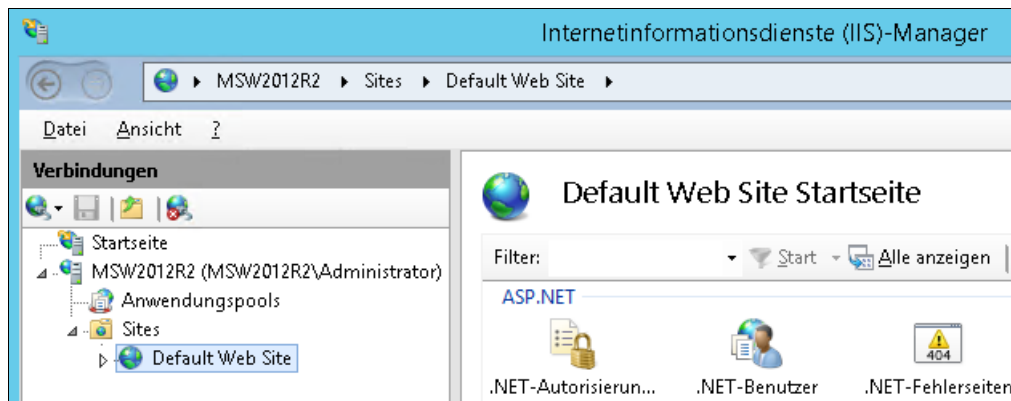
3.4.5 Setting up the URL for Certificate Revocation List – CRL

If a self-signed CA certificate is used within CompanyCRYPT for creating and signing of new certificates, then a certificate revocation list will be created automatically by CompanyCRYPT. This CRL will typically be provided via a HTTP link.

The address of the CRL consists of the domain (of the hostname) and the selected directory. Example: mail.host.com/CRL

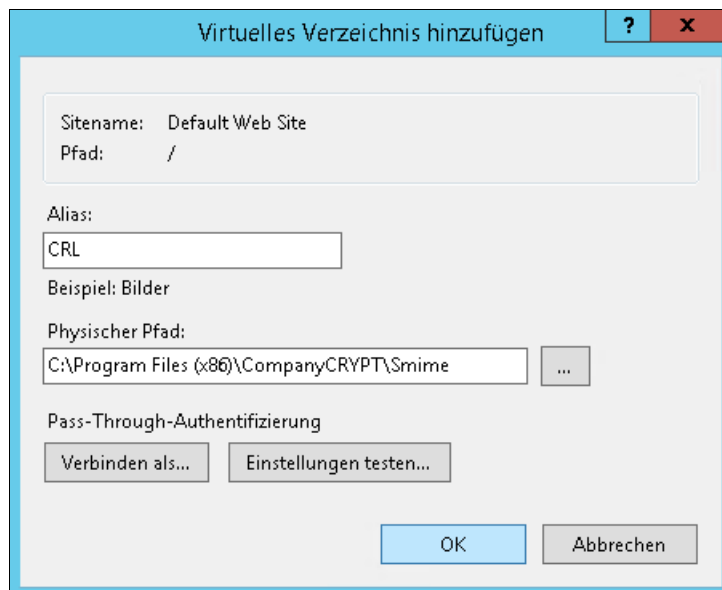
Step 1

Begin with **Start → Administrative Tools** and start the **Internet Information Services (IIS) Manager**. Move to **Internet Information Services (IIS) Manager → ... (Local Computer) → Sites** and select **Default Web Site**.



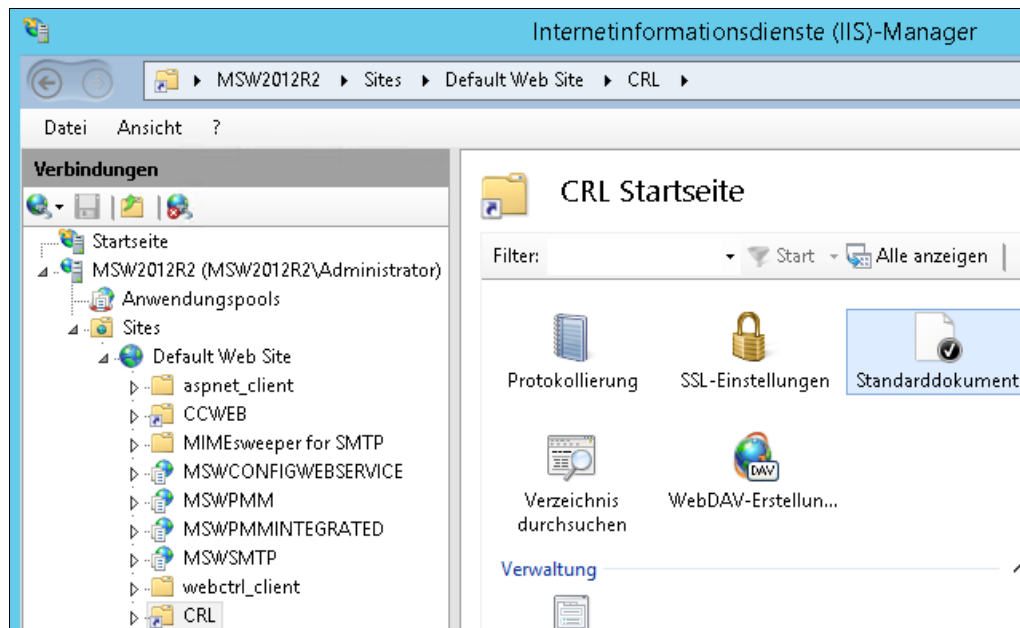
Step 2

Right-click on **Default Web Site** and select **Add Virtual Directory**. Enter **CRL** as an alias or choose an individual name. Enter the Physical path according to your installation: **<CC-Install directory>\mime** and save with **OK**.



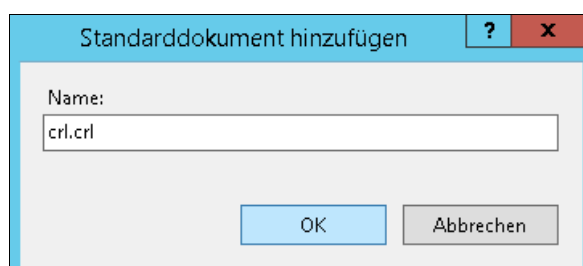
Step 3

Move to and right-click on **Internet Information Services (IIS) Manager** → ... (Local Computer) → Sites → **Default Web Site** → **CRL** → **Default Document** and select **Open Feature**.



Step 4

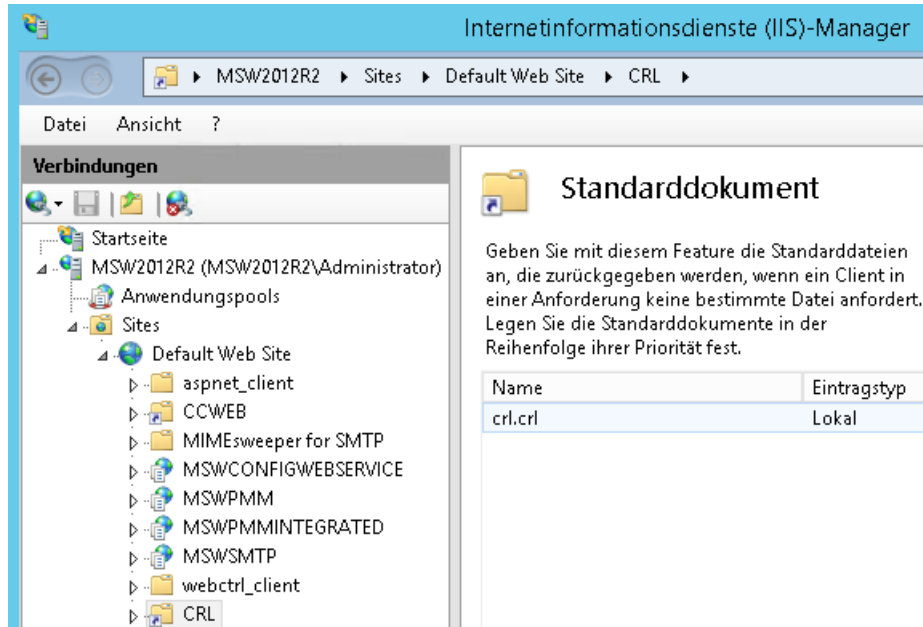
Choose the Action **Add** and enter the name **crl.crl** as the Default Document. Save with **OK**.





Step 5

Remove all entries from the list except the file name **crl.crl**.



Note: All internal certificates should contain the link to your CRL. This will provide the information about the CRL to your partners for automated queries. Full URL syntax is required. Example: <http://mail.host.com/CRL>

Important: Note that to access the Certificate Revocation List via HTTP from the Internet your firewall rules have to be modified as well.

4 De-installing CompanyCRYPT

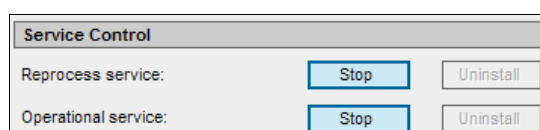
Important Note: Before de-installing CompanyCRYPT all existing CompanyCRYPT scenarios (De- and encryption jobs) have to be deleted in the MIMESweeper-Policy Editor.

4.1 Deleting CompanyCRYPT services and EXE.INI entries

WebGUI → (Configuration) System → Service Control / MIMESweeper

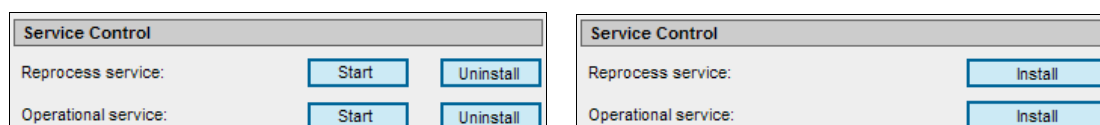
Step 1

First stop the **Operational service** by clicking on the **Stop** button. Then stop the **Reprocess Service** by clicking on the other **Stop** button.



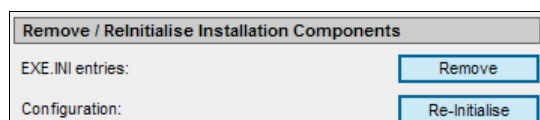
Step 2

Delete the two services by clicking on their **Uninstall** buttons. In case the button is coloured grey and you read 'Query' the stopping process is not yet complete. Refresh the display by clicking on **Query** button.



Step 3

Delete the EXE.INI entries by clicking on the **Remove** button.



Step 4

After completing step 1 through 3 you should see the view below. You may now close the WebGUI.

4.2 Remove CompanyCRYPT program files under Microsoft® Windows Server 2003

Start → Control Panel → Software → Add or Remove Programs

Step 1

Move to **Start → Control Panel → Software → Add or Remove Programs** and select the entry CompanyCRYPT, then click on the button **Remove**.

Step 2

Answer the following question „Do you really want to remove CompanyCRYPT“ with **Yes** and all program files of Company-CRYPT will be removed.

Step 3

Existing key material and files that have been modified since installation will not be removed automatically by the previous Step. If there is no longer any need for these files, the complete CompanyCRYPT can be simply deleted.

4.3 Remove CompanyCRYPT program files under Microsoft® Windows Server 2008 / 2008 R2

Start → Control Panel → Software → Add or Remove Programs

Step 1

Move to **Start → Control Panel → Programs → Uninstall a program** and select the entry CompanyCRYPT, then click on **Uninstall**.

Step 2

Answer the following question „Are you sure you want to uninstall CompanyCRYPT“ with **Yes** and all program files of CompanyCRYPT will be removed.

Step 3

Existing key material and files that have been modified since installation will not be removed automatically by the previous Step. If there is no longer any need for these files, the complete folder CompanyCRYPT can be simply deleted.

4.4 Remove CompanyCRYPT program files under Microsoft® Windows Server 2012 / 2012 R2

Start → Control Panel → Software → Add or Remove Programs

Step 1

Move to **Start → Programs and Features** and select the entry CompanyCRYPT, then click on **Uninstall**.

Step 2

Answer the following question „Are you sure you want to uninstall CompanyCRYPT“ with **Yes** and all program files of CompanyCRYPT will be removed.

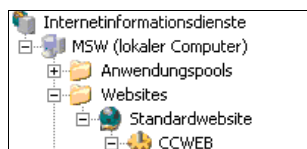
Step 3

Existing key material and files that have been modified since installation will not be removed automatically by the previous Step. If there is no longer any need for these files, the complete folder CompanyCRYPT can be simply deleted.

4.5 Remove CompanyCRYPT-WebGUI under Microsoft® Windows Server 2003

Step 1

Right-click on **Web Sites → Default Web Site → CCWEB** and select **Delete....**

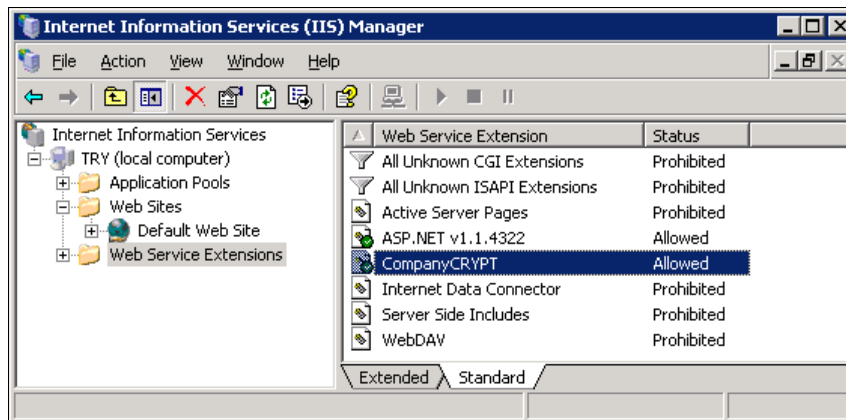


Step 2

Confirm the following question „Are you sure you want to delete this item?“ with **yes**.

Step 3

After that right-click on **Web Site Extensions → CompanyCRYPT** and select **Delete....**



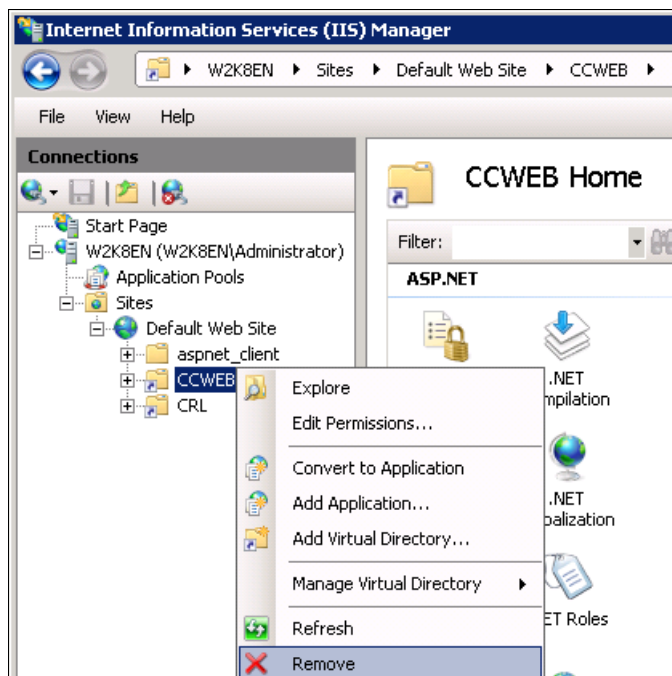
Step 4

Again confirm the following question „Are you sure you want to delete this item?“ with yes.

4.6 Remove CompanyCRYPT-WebGUI under Microsoft® Windows Server 2008 / 2008 R2

Step 1

Move to and right-click on **Internet Information Services (IIS) Manager** → ... (Local Computer) → Sites → Default Web Sites → **CCWEB** and select **Remove**.

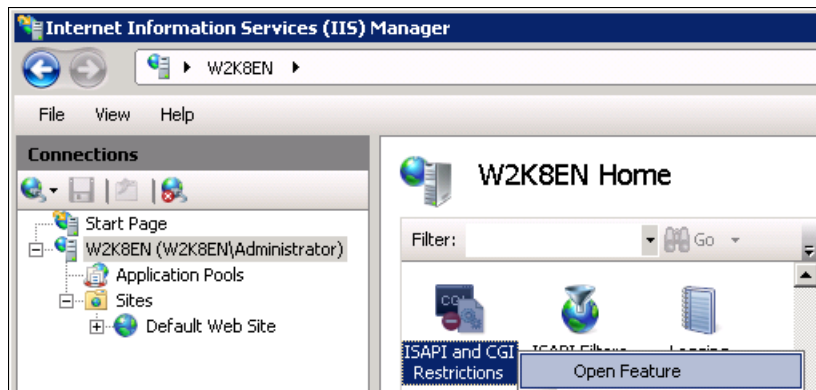


Step 2

Confirm the following question „Are you sure that you want to remove the selected virtual directory?“ with **Yes**.

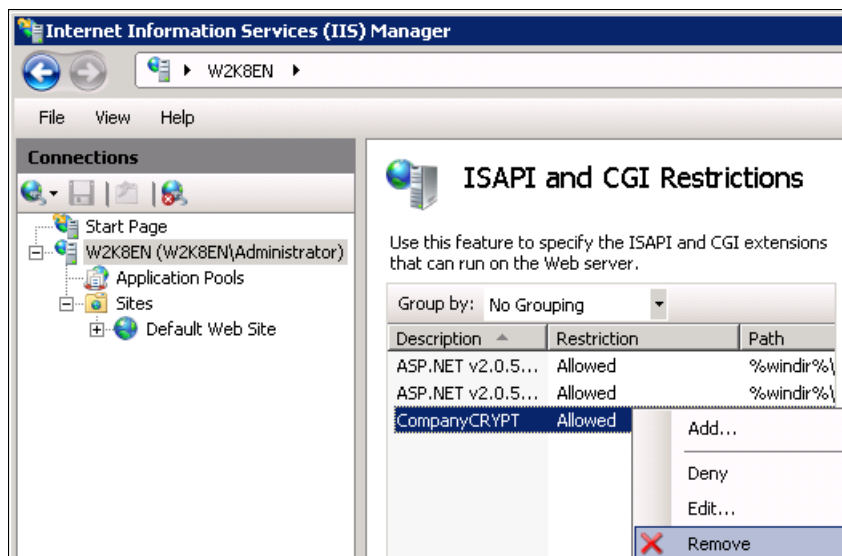
Step 3

Move to and right-click on **Internet Information Services (IIS) Manager** → ... (Local Computer) → (Features View) **ISAPI and CGI Restrictions** and select **Open Feature**.



Step 4

Right-click on the entry CompanyCRYPT and select **Remove**.



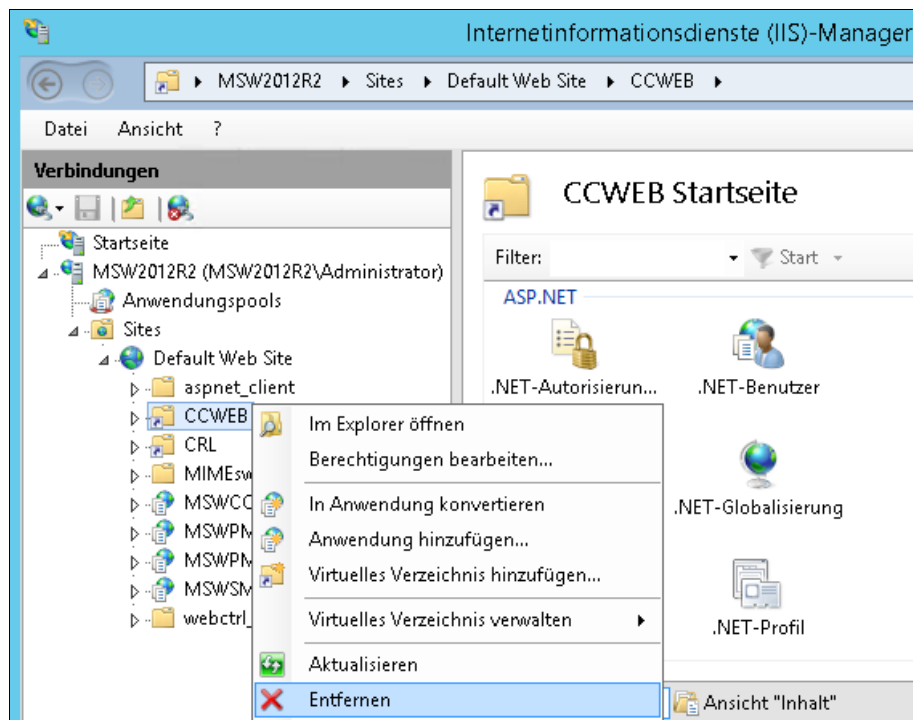
Step 5

Confirm the following question „Are you sure that you want to remove the selected restriction?“ with **Yes**.

4.7 Remove CompanyCRYPT-WebGUI under Microsoft® Windows Server 2008 / 2008 R2

Step 1

Move to the **Desktop** and start the **Server Manager**. Click on **Tools** → **Internet Information Services (IIS) Manager**. Move to and right-click on **Internet Information Services (IIS) Manager** → ... (Local Computer) → **Sites** → **Default Web Sites** → **CCWEB** and select **Remove**.

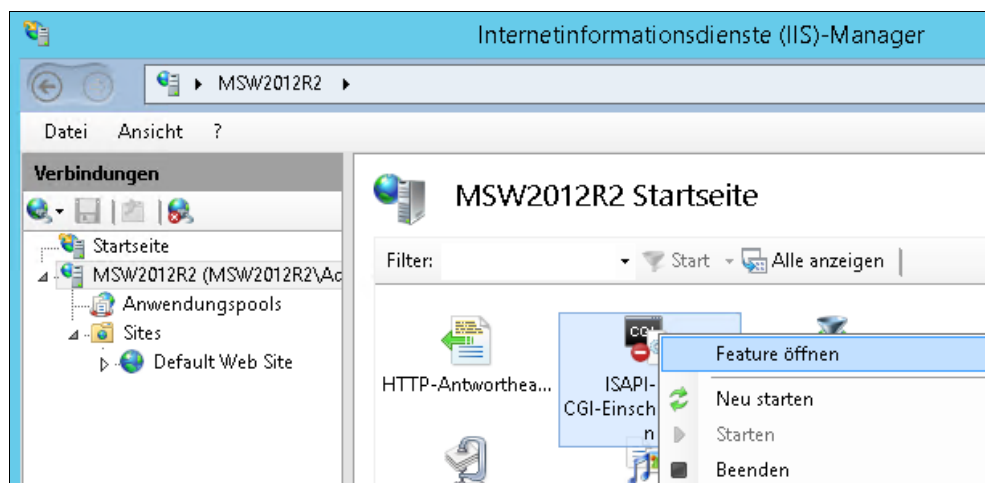


Step 2

Confirm the following question „Are you sure that you want to remove the selected virtual directory?“ with **Yes**.

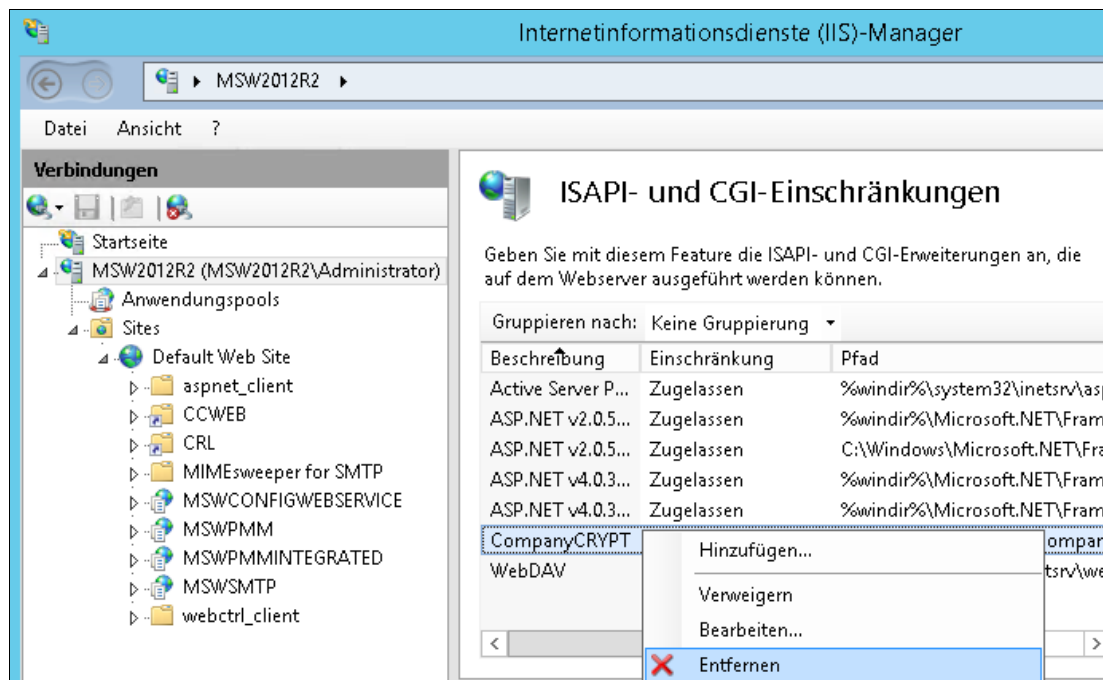
Step 3

Move to and right-click on **Internet Information Services (IIS) Manager** → ... **(Local Computer)** → (Features View) **ISAPI and CGI Restrictions** and select **Open Feature**.



Step 4

Right-click on the entry CompanyCRYPT and select **Remove**.



Step 5

Confirm the following question „Are you sure that you want to remove the selected restriction?“ with **Yes**.