TECHNICAL NOTE

Stormshield Network Firewall

AUTOMATIC BACKUPS

Document version: 1.0

Reference: snentno_autobackup

CONTENTS

snentno_autobackup - v1.0 - Copyright Netasq 2014

INTRODUCTION

Being able to count on a regular backup of your appliances is essential. Indeed, performing a periodic configuration backup (daily, weekly or monthly) makes it possible to quickly reconfigure a firewall in the event of a disaster (hardware failure, configuration error causing malfunctions, etc).

From version 1.0 of its firmware onwards, Stormshield Network's Firewalls offer the possibility of automating this backup operation in order to store output files either within the infrastructure suggested by the **Stormshield Network Cloud backup** service or on an HTTP/HTTPS server within your infrastructure.

This feature allows the administrator to be freed from having to plan configuration backups and therefore removes the risk of forgetting to perform this operation.

OPERATION

Regardless of the chosen method (Cloud backup or customized server), a local backup of the firewall's configuration will be made during any automatic backup operation. This file, named "backup.na.enc", is stored in the folder /data/Autobackup/ on the Firewall.

Storing in the Mystormshield.eu client area

When the Cloud backup option is selected, backups will be sent directly to your secure-access area (https://mystormshield.eu). The 5 most recent backups (daily, weekly or monthly) of your appliance are stored and accessible in this way.

Storing on a customized server

If you choose to store backups on a customized server, you can use the HTTP WebDAV extension (RFC 4918) to send your files. You will then need the following elements:

Microsoft Internet Information Services (IIS) server:

- Windows 2008 Server or higher,
- WebDAV,
- SSL,
- Digest or Basic authentication methods.

Apache server:

- Operating system supporting Apache (Linux, FreeBSD, etc),
- Apache modules: WebDAV (dav and dav_fs), SSL, Digest (auth_digest) or Basic (auth_basic) authentication.

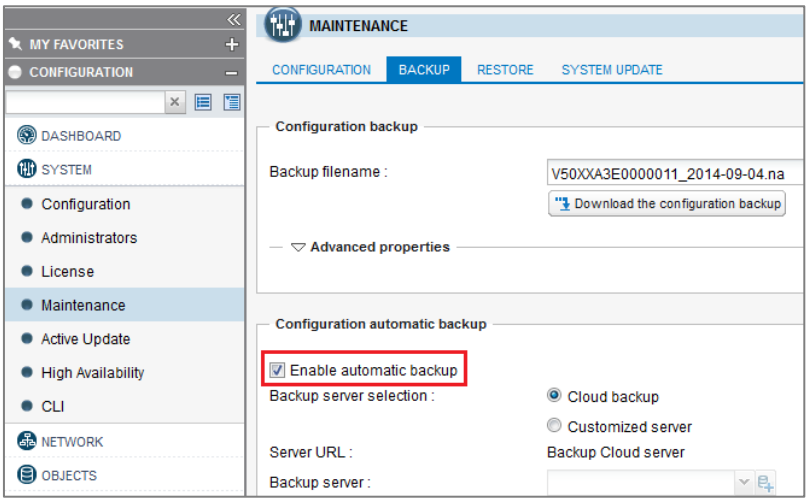
snentno_autobackup - v1.0 - Copyright Netasq 2014

FIREWALL CONFIGURATION

Activating automatic backups

Select the *Backup* tab in the module **Configuration** > **System** > **Maintenance**.

In the screen *Configuration automatic backup*, select the checkbox **Enable automatic backup**.

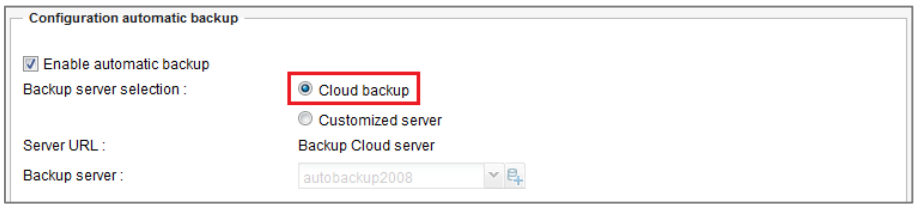


Stormshield Network Cloud Backup

In order to enable automatic backups to the **Stormshield Network Cloud backup** service, select the value *Cloud backup* for the field **Backup server selection**. Backups will then be saved in your secure-access area (https://mystormshield.eu) and identified by the firewall's serial number. For this feature, it is therefore not necessary to enter a login and password in the **Preferences** module.

NOTE

The SN Cloud Backup feature is available on all Stormshield Network Firewalls. However, the service requires the Firewall to be under a valid maintenance contract.



Only two additional fields need to be filled in:

- **Backup frequency**: select one of the 3 frequencies offered (every day, every week or every month).
- **Password of the backup file** (optional): Indicate a password that will serve to protect the backup file. You will be asked to provide this password when this file is used for the purpose of restoring a configuration.

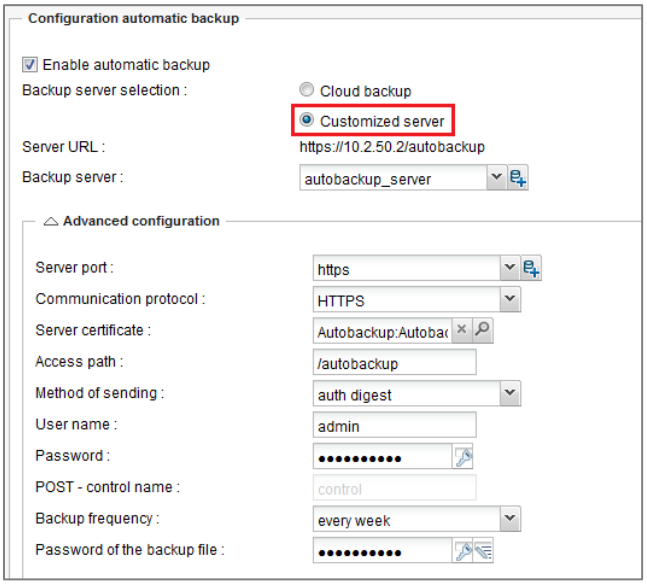
snentno_autobackup - v1.0 - Copyright Netasq 2014

Backups on a customized HTTP/HTTPS server

In the field **Backup server selection**, select the value *Customized server*. Next, fill in the various fields in the module **Advanced configuration.**

REMARK

The field **Server URL** will be entered automatically according to the values entered in the fields **Backup server**, **Server port**, **Communication protocol** and **Access path.**



Backup server

Select or create directly from this field an object representing the server to which the Firewall sends its automatic backups. If the name of the server takes the form of *server.mycompany.com* (FQDN), ensure that the firewall can indeed resolve this DNS name.

Server port

Select or create directly from this field an object representing the listening port of the backup server (port network object).

Communication protocol

Select **HTTP** or **HTTPS** (recommended) according to the protocol used on the server.

Server certificate (only if HTTPS has been selected)

Select the certificate of the backup server created or imported earlier in the firewall's PKI.

Access path

Indicate the folder of the server in which backups will be stored.

IMPORTANT

For firewalls in a firmware version lower than 1.2.0, this path has to be preceded by a "/". Example: /autobackup

snentno_autobackup - v1.0 - Copyright Netasq 2014

Method of sending

Select the access or authentication method used for placing the firewall's backups on the server (POST access control or Basic/Digest authentication for WebDAV).

The POST method does not involve any authentication. On the server side, it requires a script to process received data (saving of received files in a particular folder, etc.). This script also checks for a "control name" in the data traffic in order to process it.

The Basic identification method (RFC 2617) is unsecured by nature, as it sends the encrypted password in Base64 but in plaintext, making it easily interpretable as such. It is therefore not recommended for transferring credentials and data through an encrypted connection (HTTPS).

The Digest identification method (RFC 2617) is more secure as it is based on a "challenge/response" mechanism built around the MD5 fingerprint of the client password. Even though it can be used in HTTP traffic, you are also strongly advised to use this method through an encrypted connection (HTTPS) when transferring data.

User name (Basic or Digest methods only)

Indicate the required user name in order to connect to the server.

Password (Basic or Digest methods only)

Indicate the password of the user entered earlier.

POST – control name (POST method only)

Indicate the control name is the access method selected is POST.

Backup frequency

Select the frequency of automatic backups (daily, weekly or monthly). The first successful backup will determine the starting point for backups at the selected frequency.

Password of the backup file (recommended)

Indicate a password for protecting the backup file. You will be asked to provide this password when this file is used for the purpose of restoring a configuration.

Checking the operation of automatic backups

When the settings form is validated, an automatic backup will always be made.

Validating settings

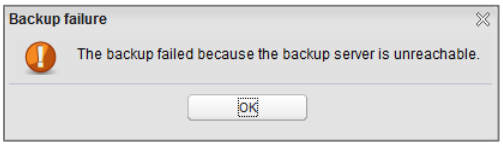
If the parameters entered are valid, the backup will be successful. The backup file will then be available on the destination server.

NOTE

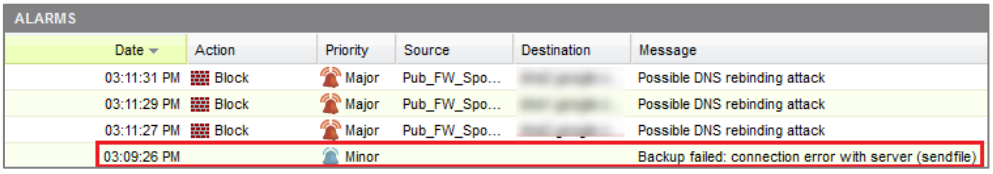
This first successful backup will determine the starting point for automatic backups at the selected frequency.

snentno_autobackup - v1.0 - Copyright Netasq 2014

However, if any of the parameters is invalid, a warning message will indicate that the backup has failed:



A message will also appear in the *Alarms* window in the **Dashboard** module:



Correct the parameter(s) in question and validate again.

Log files

When a backup is successful, logs will be saved in the file /log/l_system:

```
id=firewall time="2014-11-05 11:07:17" fw="V50XXA3E0000011"
tz=+0100 startime="2014-11-05 11:07:17" pri=5 msg="Backup
successful (local, distant)" service=sysevent alarmid=86
```

When a backup fails, logs will be saved in the file /log/l_alarm:

```
id=firewall time="2014-11-05 11:12:23" fw="V50XXA3E0000011"
tz=+0100 startime="2014-11-05 11:12:23" pri=4 msg="Backup failed:
invalid server response (sendfile)" class=system alarmid=87
```


snentno_autobackup - v1.0 - Copyright Netasq 2014

EXAMPLES OF SERVER CONFIGURATIONS

Linux and Apache

This example specifies the various stages of configuring an Apache server on a Linux platform, allowing identification in Digest mode through an SSL connection (server certificate generated through the firewall's PKI).

Installing Apache and its components

Install the various necessary components:

- Apache,
- SSL module for Apache,
- DAV module for Apache,
- dav_fs module for Apache,
- _auth_digest module for Apache.

Create the folder for receiving automatic backups (example: */var/www/html/autobackup*).

SSL settings

Creating the server certificate

On the firewall hosting the CA used for automatic backups, create a server certificate relating to the server hosting the backups (module **Configuration** > **Objects** > **Certificates and PKI**).

Next, select the certificate created and export it in PKCS12 format (menu **Download** > **Certificate as a P12 file**).

Importing the certificate on the Apache server

Submit the PKCS12 file on the server and proceed to extract the private key and certificate.

Use the following command to extract the private key:

```
openssl pkcs12 -in server_certificate.p12 -nocerts -nodes -out server_key.key
```

REMARK

The option "-nodes" must be removed from the line if you wish for the private key to remain password-protected. However, in this case, you will be asked to provide this password every time the Apache server reboots.

Use the following command to extract the certificate:

```
openssl pkcs12 -in server_certificate.p12 -clcerts -nokeys -out server_certificate.crt
```


snentno_autobackup - v1.0 - Copyright Netasq 2014

Next, move the certificate and private key to their respective folders (example: */etc/pki/tls/certs* and */etc/pki/tls/private*). Restrict privileges on the private key to only the superuser (example: `chmod 400 /etc/pki/tls/private/server_key.key`).

Adapt the SSL configuration file accordingly (example: */etc/httpd/conf.d/ssl.conf*):

```
#   Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate.  If
# the certificate is encrypted, then you will be prompted for a
# pass phrase.  Note that a kill -HUP will prompt again.  A new
# certificate can be generated using the genkey(1) command.
SSLCertificateFile /etc/pki/tls/certs/server_certificate.cert

#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile /etc/pki/tls/private/server_key.key

#   Server Certificate Chain:
#   Point SSLCertificateChainFile at a file containing the
#   concatenation of PEM encoded CA certificates which form the
#   certificate chain for the server certificate. Alternatively
#   the referenced file can be the same as SSLCertificateFile
#   when the CA certificates are directly appended to the server
#   certificate for convinience.
#SSLCertificateChainFile /etc/pki/tls/certs/server-chain.crt
```

Configuring WebDAV

After having installed the dav, dav_fs and auth_digest modules, create a WebDAV configuration file for Apache (Example: */etc/httpd/conf.d/webdav.conf*) containing the following directives:

```
# DIGEST method
Alias /autobackup /var/www/html/autobackup
<Directory "/var/www/html/autobackup">
                Dav On
                Order Allow,Deny
                Allow from all

                AuthType Digest
                AuthName "Autobackup"
                AuthUserFile "/etc/httpd/user.passwd"
                AuthDigestProvider file

                Require valid-user
</Directory>
```

In the example shown:

- The server can be contacted at the address *https://server_name/autobackup* (**Alias** directive pointing to the physical folder */var/www/html/autobackup*).
- The authentication domain (Realm) is *Autobackup* (**AuthName** directive).
- The authentication method used is Digest (**AuthType** directive).

snentno_autobackup - v1.0 - Copyright Netasq 2014

- The login/password pairs allowed to access this folder are stored in the file */usr/local/www/user.passwd* (**AuthUserFile** directive).

Next, create the password file for Digest mode and the first account (*Autobackup* authentication domain and the user *autobackup* in the example) using the command:

```
htdigest -c /usr/local/www/user.passwd Autobackup autobackup
```

Enter the user's password upon the command invite.

Subsequently, if you wish to add other access accounts (new_account in the example), use the following command:

```
htdigest /usr/local/www/user.passwd Autobackup new_account
```

Start or restart the Apache server to apply all changes.

Windows 2008 Server and IIS

This example sets out the various steps in configuring an IIS server on Windows 2008 Server, allowing identification in Digest mode through an SSL connection (server certificate generated through the firewall's PKI).

NOTE

In order to enable SSL in IIS, the server has to be a member of an Active Directory domain.

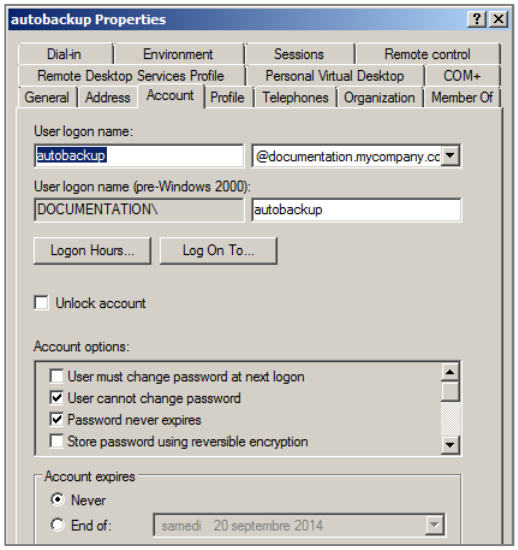
Using the Windows file explorer, create the folder meant for receiving automatic backups (example: *c:\inetpub\wwwroot\autobackup*).

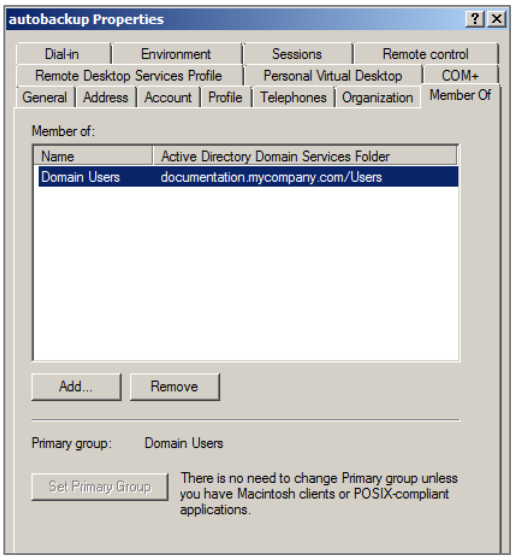
User account for backups

Create a dedicated user for automatic backups in the Active Directory Users and Computers console.

In this example, the account used is named *autobackup* and belongs to the *Autobackup Allowed Users* group specifically created for this purpose. Writing privileges on the folder dedicated to backups can be defined in the settings of the Webdav site.

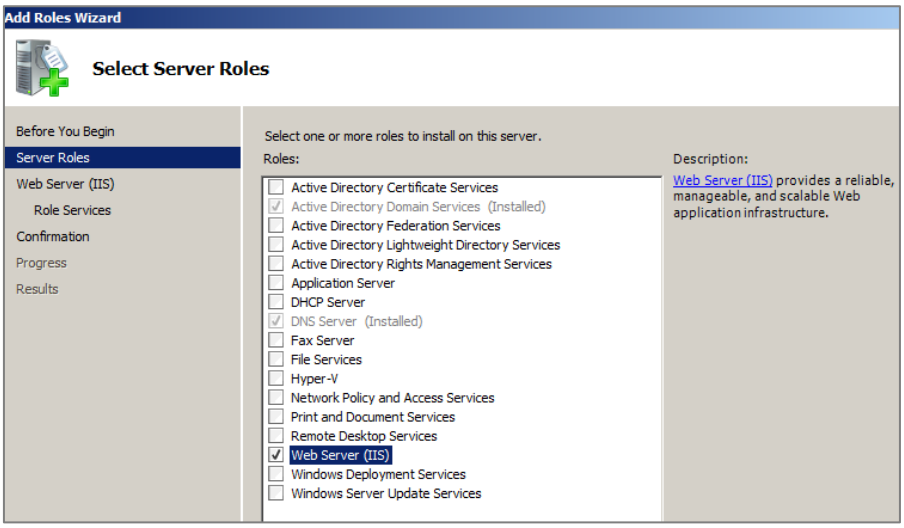
snentno_autobackup - v1.0 - Copyright Netasq 2014





Installing IIS and its components

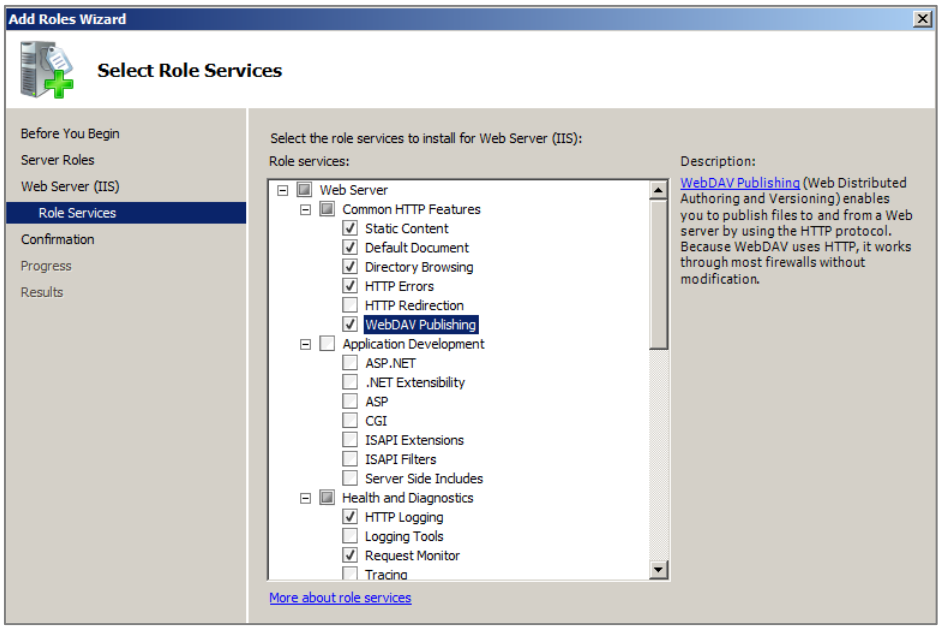
If it has not yet been installed, add the IIS role in the Server Manager console (menu **Add roles** > **Server roles** > **Web Server (IIS)**).



During the installation of the IIS role, or when selecting the option **Add Role service** for the **Web Server (IIS)** role in the Server Manager console, select the following options:

Web Server
- Common HTTP Features
  - WebDAV Publishing
- Security
  - Basic Authentication
  - Digest Authentication
- Management Tools
  - Management Service

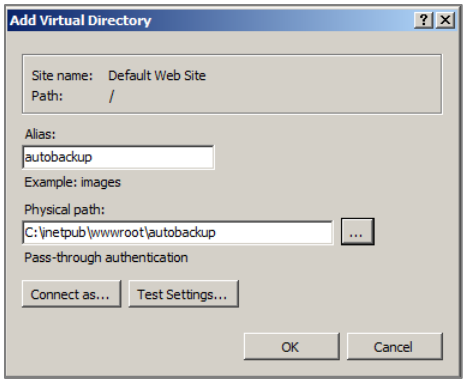
snentno_autobackup - v1.0 - Copyright Netasq 2014



Creating a virtual folder

In this example, the site used for receiving and storing backups will not be the *Default Web Site*, but a dedicated site named *autobackup*, whose base folder will be located under the root of the *Default Web Site* (*c:\inetpub\wwwroot*).

Launch the Internet Information Server (IIS) Manager console. Right-click on **Default Web Site** and select the option **Add Virtual Directory**.

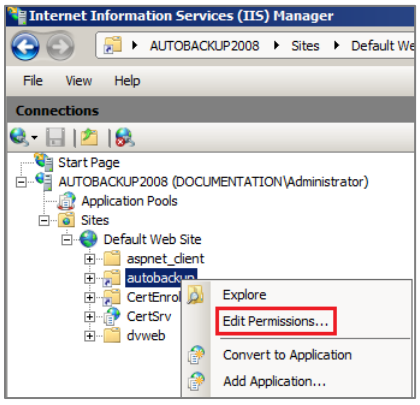


In the field **Alias**, select the name given to your site (example: *autobackup*); the address of the site will take the form *https://server_name.company.com/alias*.

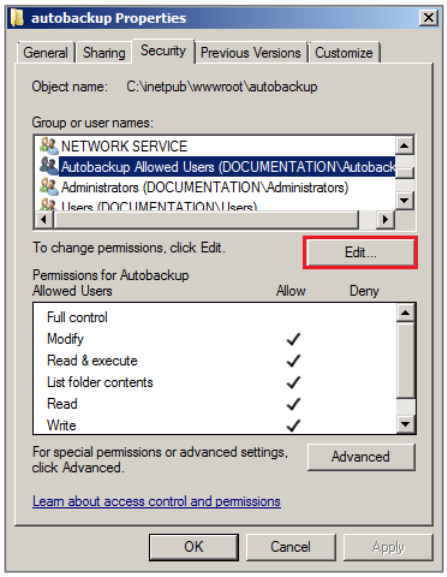
In the field **Physical path**, select (or create) the physical folder corresponding to your virtual site (example: *c:\inetpub\wwwroot\autobackup*).

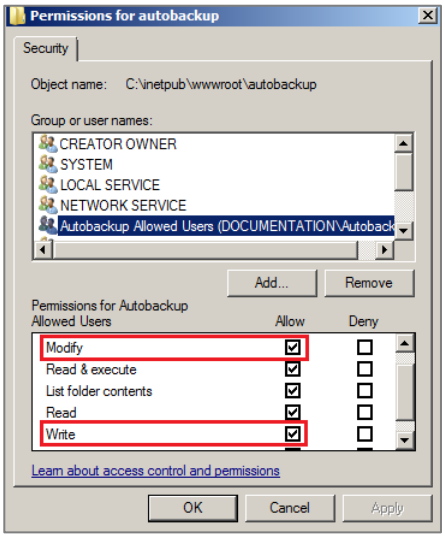
Next, grant writing privileges on the physical folder meant for storing the backups of the group of dedicated users. To do so, right-click on your site and select the option **Edit Permissions** in the pop-up menu.

snentno_autobackup - v1.0 - Copyright Netasq 2014



In the *Security* tab, click on **Edit**. Select the user group (example: *Autobackup Allowed Users*) and select the checkboxes **Modify** and **Write**, then validate.





Directory browsing privileges

In the Internet Information Server (IIS) Manager console, select your site (*autobackup* in the example) and double-click on the **Directory browsing** icon.

In the right panel (*Actions*), click on **Enable.**

Adding a MIME type for backup files

Backup files are encrypted and have an ".enc" extension. Since this extension is unknown to the IIS server, it must be defined so that the server will know which action to perform when you click on the link corresponding to a backup (execute the file, suggest opening or downloading it, etc.).

In the *Internet Information Server (IIS) Manager* console, select your site (*autobackup* in the example) and double-click on the **MIME Types** icon.

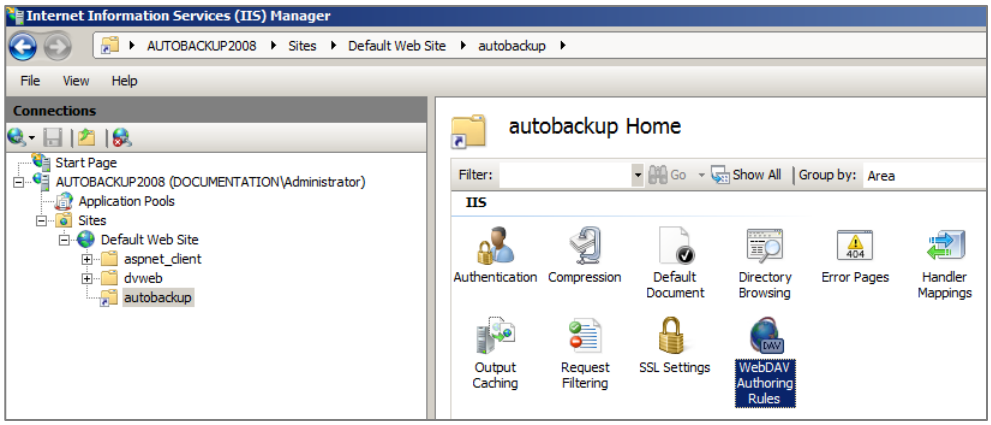
snentno_autobackup - v1.0 - Copyright Netasq 2014

In the right panel (*Actions*), click on **Add**. In the field **File name extension**, indicate *.enc*. In the field **MIME type**, specify *application/octet-stream*.

Configuring WebDAV

Enabling WebDAV

In the *Internet Information Server (IIS) Manager* console, select le site *Default Web Site* and double-click on the **WebDAV Authoring Rules** icon.



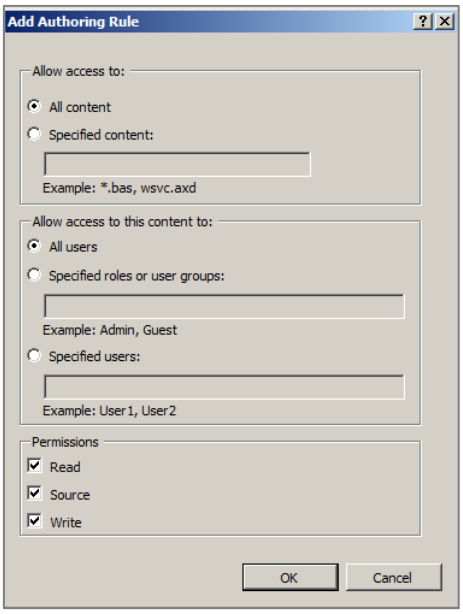
In the right panel (*Actions*), click on **Enable WebDAV**:

Rules for creating WebDAV

In the IIS console, select your site (*autobackup* in the example) and double-click on the **WebDAV Authoring Rules** icon.

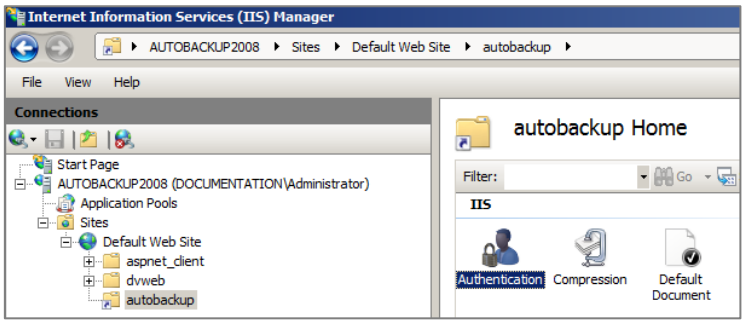
In the right panel (*Actions*), click on **Add Authoring Rule…** For this rule, select the options **All content**, **All users** and **Permissions: Read, Source, and Write**.

snentno_autobackup - v1.0 - Copyright Netasq 2014

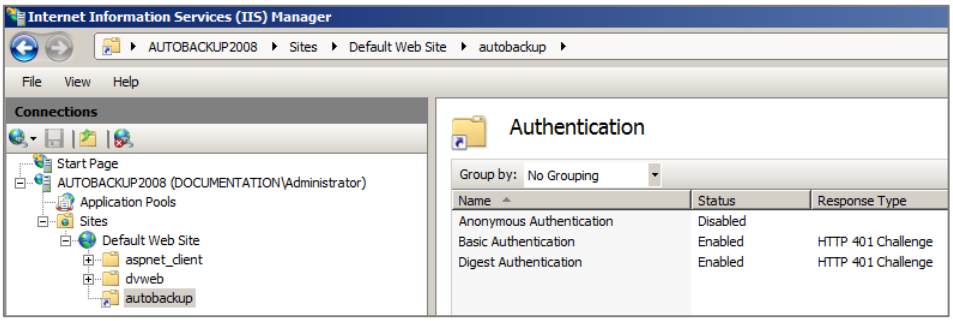


Authentication

In the *Internet Information Services Manager* console, click again on your site and double-click on the **Authentication** icon.

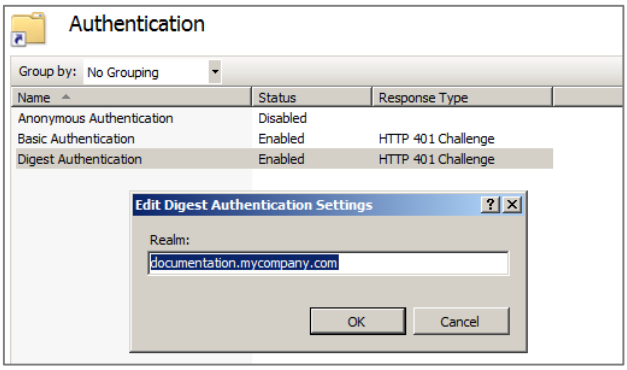


Enable **Basic Authentication** and **Digest Authentication**, and disable **Anonymous Authentication**.



Select **Digest Authentication** and click on **Edit** in the right panel to specify the server's Active Directory domain (*documentation.mycompany.com* in the example).

snentno_autobackup - v1.0 - Copyright Netasq 2014



SSL settings

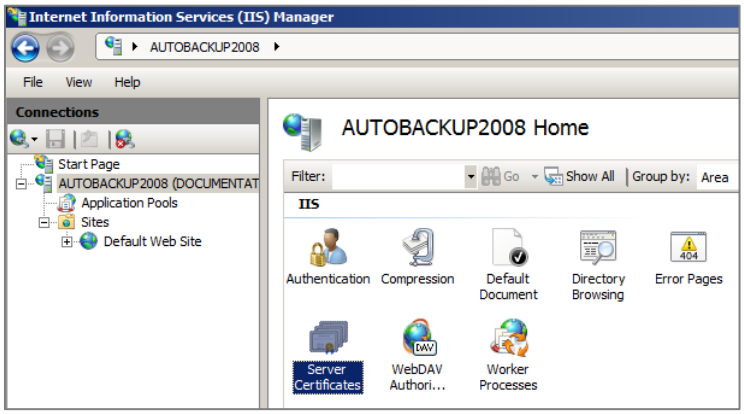
Creating the server certificate

On the firewall hosting the CA used for automatic backups, create a server certificate relating to the server hosting the backups (module **Configuration** > **Objects** > **Certificates and PKI**).

Next, select the certificate created and export it in PKCS12 format (menu **Download** > **Certificate as a P12 file**).

Importing the certificate on the IIS server

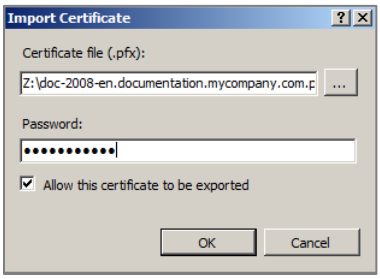
In the *IIS Manager* console, select the name of the server and double click on the option **Server Certificates**.



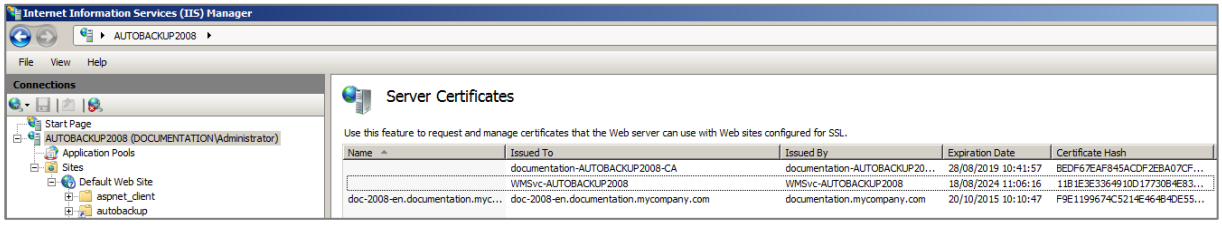
In the right panel (*Actions*), click on **Import.**

Select the certificate exported earlier and enter the associated password.

snentno_autobackup - v1.0 - Copyright Netasq 2014



The certificate will then appear in the IIS certificate store:



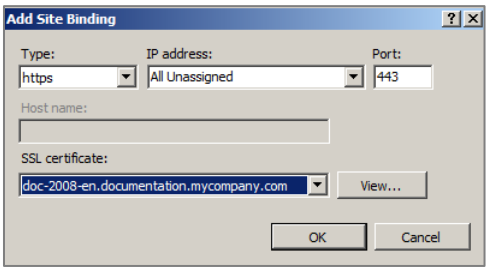
In the *IIS Manager* console, click again on the *Default Web Site* then select the option **Bindings** in the right panel. Add a link with the following values:

Type: https

IP address: the IP address on which the server has to be contacted in HTTPS

Port: 443

SSL certificate: the certificate imported earlier.



Exclusive access in SSL

In this case, this refers to the exclusive authorization of access in SSL to the backup storage server.

In the *IIS Manager* console, click on your site and double-click on the icon **SSL Settings.** Select the checkbox **Require SSL** and apply.

snentno_autobackup - v1.0 - Copyright Netasq 2014