

Configure SafeConsole server



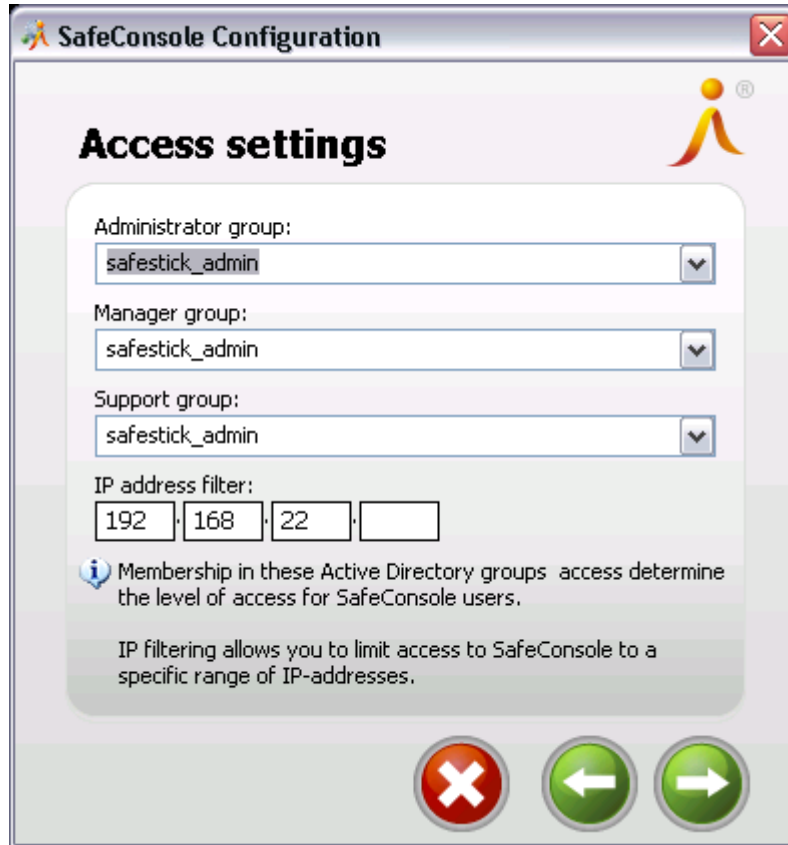
The screenshot shows the 'SafeConsole Configuration' window with the 'Domain settings' tab selected. The window contains the following fields and options:

- Domain name:** A text box containing 'gestur.local'.
- Domain controller:** A text box containing 'dom1.gestur.local'.
- Non-privileged AD user:** A text box containing 'administrator'.
- Password:** A password field with 10 dots.
- This domain has an integrated Exchange server
- Information icon:** A blue 'i' icon next to the text: 'SafeConsole needs a user name and password to interact with the Active Directory.'
- Help text:** 'If an integrated mail server is used, SafeConsole assumes that an e-mail address has the form user@domain.server unless specified in the Active Directory.'
- Navigation buttons:** A red 'X' button (Close), a grey left arrow button (Previous), and a green right arrow button (Next).

When the configuration starts you will see your domain name in the top field and your primary domain controller in the net field. If you are installing SafeConsole on a computer that is not part of the domain you will have to manually enter these fields.

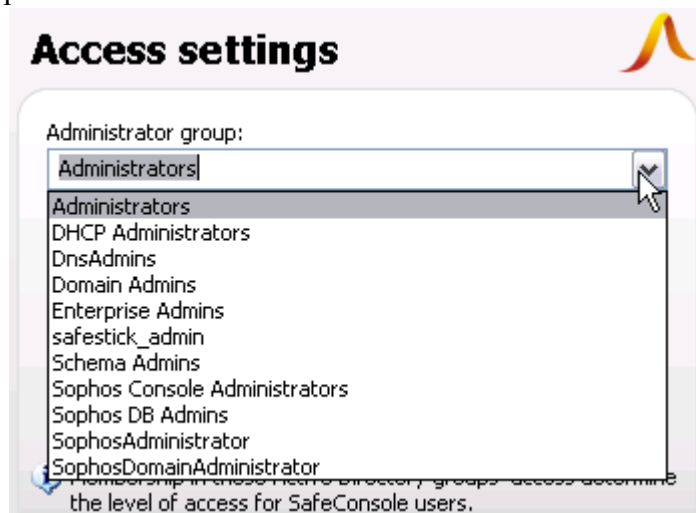
1. Enter the credentials of a domain user, preferably not an administrator. This is to access the Active Directory
2. Check or uncheck the integrated Exchange server box. Leaving it unchecked means that email addresses will have to be registered from each users SafeStick when password recovery is activated
3. Click next

If a successful connection to your AD is made you will see the next screen, otherwise a message will appear stating that the connection failed.



In the access settings, decide what security groups in Active directory that will have access to the SafeConsole. Administrators will be able to install new certificates and licenses and all other actions, managers will only be able to change and create settings for the SafeStick drives functionality. The support group will only be able to generate lost password recovery codes for SafeStick users.

1. Start typing the first letters in the security group you wish to use for administrators
2. expand the drop down:



3. choose the preferred group. Repeat for managers and support
4. Enter the preferred Ip address filter for access to the console user interface. This is primarily to stop intruders to log in from the outside world when SafeConsole is published externally. If you do not want to restrict access by Ip addresses, leave the fields blank.



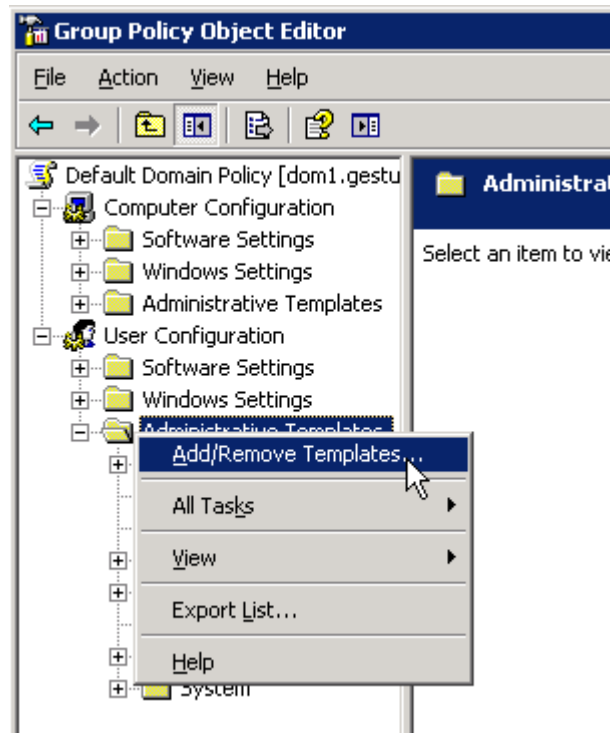
Choose an SSL certificate to identify the server and encrypt the communication. If you have your own CA you may issue a SSL certificate from it. The advantage of this is that the SSL certificate chain will be trusted on all clients. The subject must correspond the the server url.

1. Click import or generate certificate.
2. Choose a password for the PKCS12 file
3. Verify that the server address is correct.
4. Click next

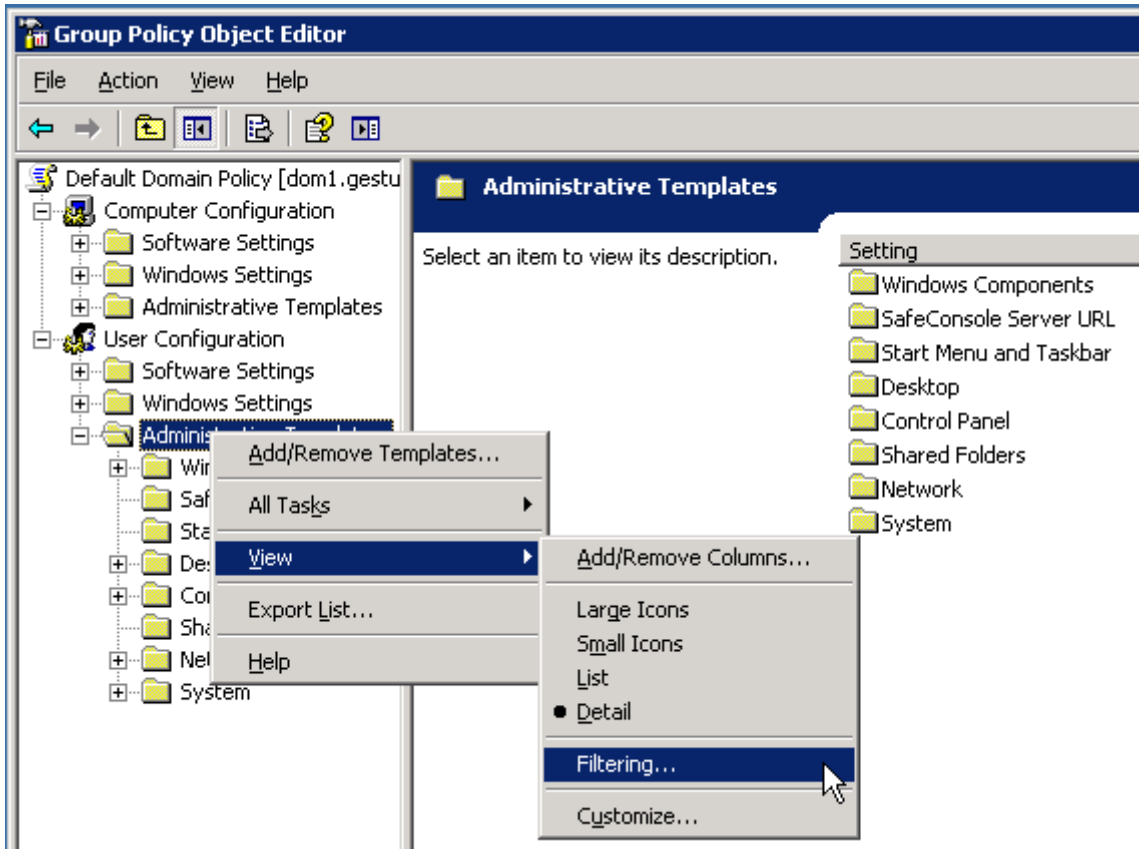
The SafeConsole is now started and will synchronize with Active Directory automatically. You may log in to SafeConsole using from a web browser and your Windows user credentials provided you are a member of one of the above mentioned security groups.

Deploying to clients

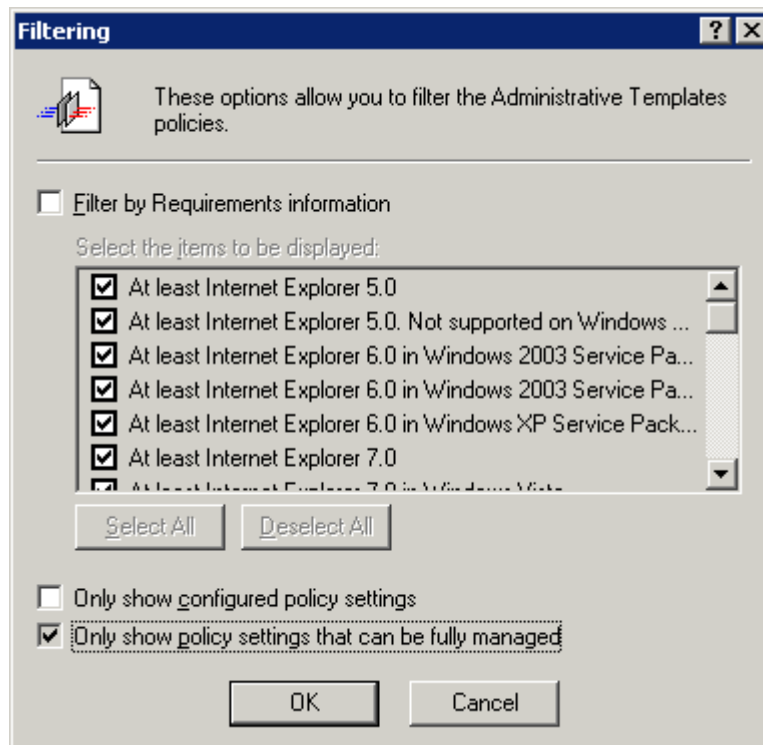
1. collect the two files:
safeconsole.adm in the [SafeConsole installation]\resources\ directory
keystore.p12 from the [SafeConsole installation] directory
2. Open your GPO editor to your domain controller, you may create a new GPO or use an existing



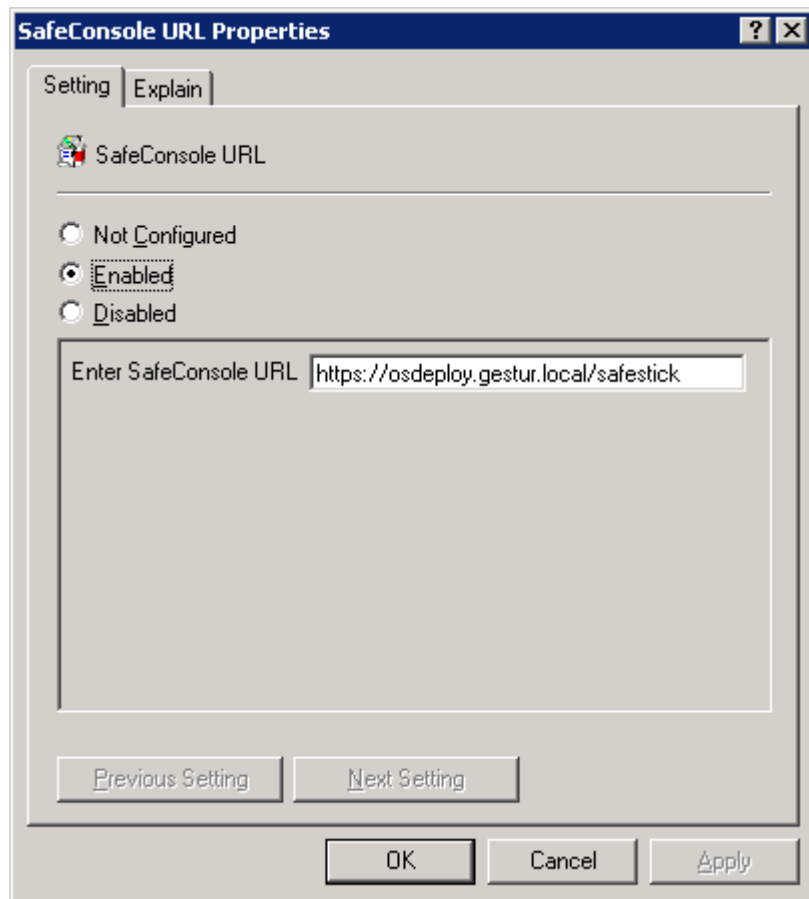
3. Import the safeconsole.adm file in your User settings – administrative templates



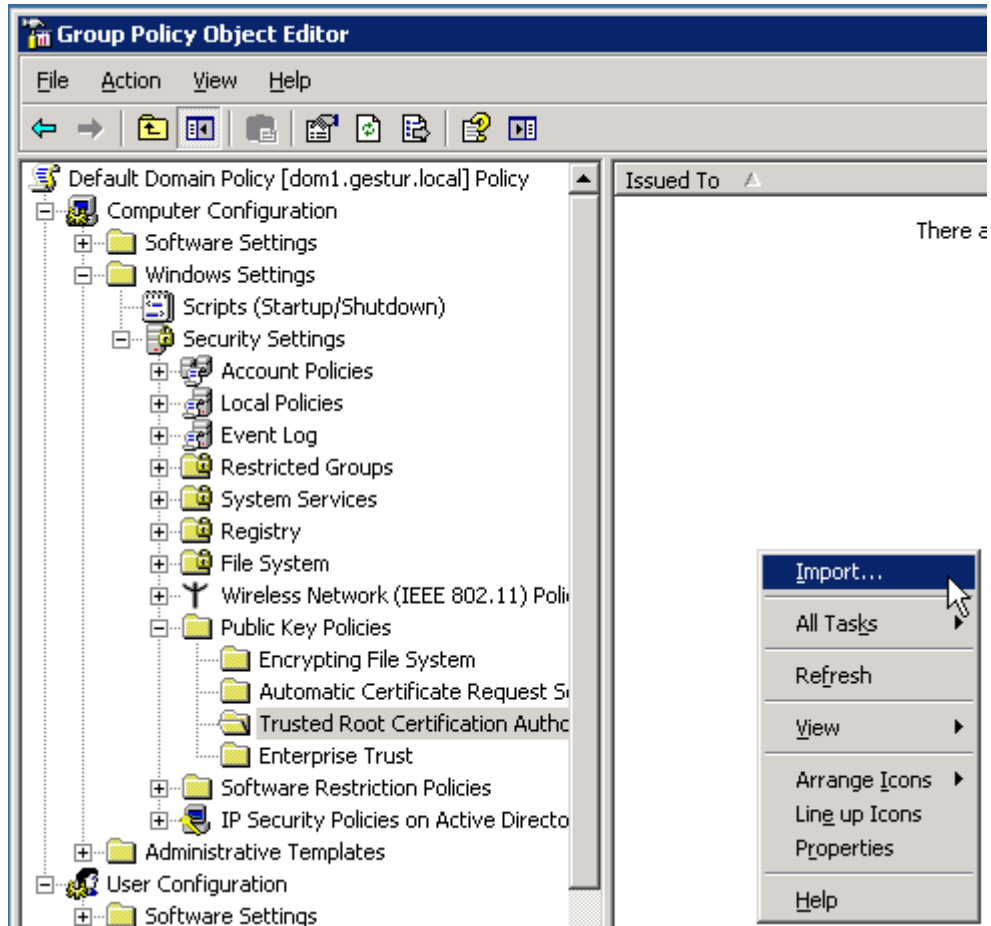
4. Right click on the administrative template and choose: 'view' – 'filtering'
5. Uncheck the check box 'only show policy settings that can be fully managed'



6. choose 'enable' on the SafeConsole URL, you should see the server URL:port/SafeStick



7. Go to 'Computer Configuration' - 'Windows settings' – security settings – 'public key policies' – 'trusted root certification authorities'



8. Choose import certificate, browse to you keystore.p12 file and enter the password
9. Make sure the GPO is distributed to the clients