Access Control

Table of Contents

How to register a new operator in ADSS Server?

Prerequisites:

Access to ADSS Server Console is over SSL Client Authentication. Operators that require access to the ADSS Server Console must have a valid certificate from:

- An external CA (trusted in ADSS Server).
- Generated within the ADSS Server Key Manager module by locally certifying the key (if this option has been allowed in the license file).
- By sending the operator's certificate PKCS#10/ CSR to an external CA for certification.

The key and certificate are usually held in a PKCS#12/ P12/ PFX file, and protected by a passphrase. However, the USB and smartcard tokens can also be used with their PINs. A matching certificate file (.cer) will also be required during registration.

Steps:

To register a new operator/ Administrator for ADSS Server console, the existing operator should:

- Define the CA that issued the certificate for the operator within the Trust Manager module and ensure it has an additional property of "CA for verifying SSL client certificates".
- Browse Access Control > Manage Operators, create a new operator, set their role and register their certificate (.cer) generated using the above mentioned steps.
- Import the PFX file of the new operator in the browser key-store of the machine (or in the USB and smart card token), from where the ADSS Server console should be launched.
- Restart the ADSS Server console component Windows service or Unix daemon for the changes to take effect.

However, if a new ADSS Server administrator / operator does not require formal access to the ADSS Server console, and just looking to receive the email alerts, then the existing operator should:

- Browse Access Control > Manage Operators, create a new operator and set their role, but ignore the field requesting the operator certificate (.cer).
- Restart the ADSS Server console component Windows service or Unix daemon for the changes to take effect.

How to login to the ADSS Server Console if the admin operator SSL/TLS client authentication certificate has expired?

If all Admin/ Operator client authentication certificates for ADSS Server have expired then access to the ADSS Server console can be recovered using this recovery option:

1. Download this special utility from the following link depending on the ADSS Server version:
   a. ADSS Server v3.6 and earlier: https://account.ascertia.com/downloads/misc/certrenewalutil/ADSS-Server-v3.6-&-Prior-AdminCertRenewal.zip
   b. ADSS Server v3.7 to v4.2: https://account.ascertia.com/downloads/misc/certrenewalutil/ADSS-Server-v3.7-to-v4.2-AdminCertRenewal.zip
   c. ADSS Server v4.3 to v4.7.4: https://account.ascertia.com/downloads/misc/certrenewalutil/ADSS-Server-v4.3-to-v4.7.4-AdminCertRenewal.zip
   d. ADSS Server v4.7.5 and later: https://account.ascertia.com/downloads/misc/certrenewalutil/ADSS-Server-v4.7.5-&-Later-AdminCertRenewal.zip
2. Stop the ADSS Server Console service.

3. Take a backup of [ADSS-Server-Installation-Dir]\conf and [ADSS-Server-Installation-Dir]\setup directories.
4. Extract the zip and overwrite its contents on the [ADSS Server Installation Directory] directory.
5. Open the command prompt and go to the directory [ADSS-Server-Installation-Dir]\setup\
6. Execute the command “**bin\renew_admincert.bat**"
7. Start the ADSS Server Console service
8. Install the new PFX: [ADSS-Server-Installation-Dir]\setup\certs\adss_default_admin.pfx in your browser to login to the ADSS Server Console. The PFX password is: password
9. Access the ADSS Server Console from your browser and go to Global Settings > System Certificates module and click the Update button.
   NOTE: If the SSL Server Authentication Certificate has also expired then follow the link to configure the new certificate: http://kb.ascertia.com/display/ADSS/Configuring+SSL+Authentication#ConfiguringSSLAuthentication-HowtoreplacethedefaultADSSSSLServerAuthenticationCertificatewithaproductioncertificate?
10. Restart the Core, Console and Services again for the changes to take effect.
11. You should remove the old expired default Admin SSL client authentication certificate from your browser key stores to avoid any confusion

> ⓘ IMPORTANT: This default admin certificate should never be used in a production environment, it is simply provided for boot-strapping and testing purposes, and must be replaced with production certificate (and associated cryptographic keys) generated by the ADSS Server operators as soon as possible.

How to ensure the accessibility of ADSS Server Console?

ADSS Server depends upon a number of external agents for its console to work properly, i.e. ADSS Server service/ daemon, Database, HSM, Ports, SSL Client certificate, disk size, etc. If any of these are not configured properly, then ADSS Server console may become inaccessible.

To ensure the accessibility of ADSS Server console:

- Ensure that the ADSS Server Windows (or Unix) service for Console component is running, where the ADSS Server Console is installed. By default, ADSS Server Console runs on port 8774.
- Access the ADSS console through any Internet browser from the machine where ADSS Server Console is installed, by specifying address: https://localhost:8774/adss/console. This should display a webpage with details of running services on ADSS Server.
- If ADSS Server is configured to run behind a DMZ then ensure the SSL port is open on the front end web server (IIS, IBM HTTP Server) for the incoming Client SSL requests. Also, ensure that the Root CA of the SSL Client certificate is trusted by the front-end web server.
- Ensure the operator’s SSL Client Authentication certificate is installed on the client's machine browser.
- Ensure the DBMS is running and is accessible from the ADSS Server machine.
- If the SSL Server Authentication keys for your ADSS Server resides in an HSM then ensure the HSM is available.
- When upgrading, the installation might be re-calculating HMACs on the basis of a number of records in the transaction table, so it could take some time to access ADSS Server console.
- Ensure sufficient disk space is available where ADSS Server is running, e.g. +50MB.
- Ensure sufficient disk space is available where the DBMS is running, e.g. 100MB.
- After confirming the above mentioned checks, restart the service/ daemon, and if this does not work restart the machine.

Why can't I access the ADSS Server administration console using Internet Explorer?

If you are unable to access the ADSS Server Console using Internet Explorer but other browsers are working, then check these aspects:

1. Ensure that you have imported the ADSS Server admin PFX in your Web browser i.e. Internet Explorer.
2. Ensure that Internet Explorer **Security level** is not set to High:
   - **Launch** the Internet Explorer
   - Go to **settings > internet options**
   - Navigate to **Security tab**
   - Ensure that preferred **Security level** is set to **Medium-high**, If it is required to run the Internet Explorer under **High Security level**, then you need to perform these steps (It may not work on some versions of IE):
     - Under the security tab click on the **Custom Level** button
     - Enable the following options:
       - Scripting for Java Applets
       - Active Scripting
3. Ensure that the ADSS Server **Machine Name or IP** must be used as the **Common Name** as well as in the **SAN extension** of the SSL Server Authentication Certificate. In case you are using default ADSS SSL Server Authentication Certificate then click here for instructions to replace it.
4. Contact support@ascertia.com if everything looks okay but the Console remains inaccessible on Internet Explorer.

How to use the "Security Officer" role to implement "Dual Control"?

"Security Officer" is a default role that has privileges to access the "Approval Manager" module in ADSS Server, and give approvals for the operations that are configured as "dual control". When dual control is enabled (from Access Control > Manage Roles) for any configurable operation, it implies that when one operator/ administrator configures that operation (i.e. creates / edits / deletes), the same operation will have to be reviewed and approved by the Security Officer to become effective. These operations will not be effective in ADSS Server, until approved by the Security Officer. In this way, it is ensured that critical changes cannot be effective without the consent of two suitably privileged staff members.

Moreover, Security Officers cannot approve their own operations to ensure that dual control is preserved in all cases. The Security Officer may also perform other configurations on ADSS Server, depending on the privileges assigned to him. However, if there is no as such requirement, then these additional privileges should not be assigned to Security Officer. See details to learn more about the Approval Manager module and Dual control feature.

How to prevent revoked operators to login to ADSS Server Console?

In order to prevent operators to login with revoked certificate:

- Turn on revocation checking for the operators' certificates. This can be done from Global Settings > Miscellaneous Settings> Revocation Settings area.
- Once enabled, the revocation checking for the operators' certificates will be performed on the basis of the configured validation policy of the CA certificate which has issued the certificate(s) to the operator(s).

  In this way, ADSS Server won't allows the operators with revoked certificates to login.

> ⓘ The access rights and role of an ADSS Server's operator is defined by the Access Control module. If you wish to manually prevent an operator from being able to login, simply set their status to INACTIVE. It is not a good idea to delete operators because their details are recorded in operational logs.

How can I update my user certificate which is about to expire?

If you see an alert message on the home page of ADSS Server Console indicating such as **1 ADSS Server operator certificates will expire within 30 days. Import new certificate within Access Control module to avoid login problems.**

This issue can be resolved by doing this:

1. Get a new SSL client authentication certificate from your CA - or If the CA is configured in the ADSS Server then generate a new key in Key Manager and certify this with the purpose SSL Client Authentication and then export the PFX and certificate to the local system.
2. Install the new key (PFX) in MSCAPI (for IE and Chrome) or NSS Keystore (for Firefox)
3. Go to the home page and click the "1 ADSS Server operator certificates will expire within 30 days. Import new certificate within Access Control module to avoid login problems." alert. It will take you to the **Access Control > Manage Operators** module and show the user(s) for which the certificate is about to expire.
4. Edit the user for which you wish to update the certificate.
5. Import the new certificate using the **Browse** option and Update the settings.
6. Relaunch the browser by closing all browser instances.
7. Access the ADSS Server Console using the new certificate, the message will no longer be shown.

How can I delete the default admin operator?

1. Launch the ADSS Server Console
2. Navigate to location **Access Control > Manage Operators**
3. Select the admin operator and clicking on the **Delete** button will remove the operator from database permanently if it is never used to login the ADSS Server Console.

   > ⚠ If the operator ever logged the ADSS Server Console even once then the operator's status will be marked as DELETED in the database and operator will not be shown in the operator's list. By doing so, another operator registration will be allowed in the license.

How can I recover the deleted operator?

1. Launch the ADSS Server Console
2. Navigate to location **Access Control > Manage Operators > Search**
3. **Search** the deleted operator
4. Click on **Operator ID** link in the list
5. Select **Active** status from dropdown
6. Click the **Update** button to complete the operation

If the license allows registering another operator only then you would be able to activate a deleted operator