ADSS OCSP Server – Quick Guide

This document aims to provide a quick ‘do this and it works’ guide to evaluating ADSS Server as an Enterprise or Infrastructure class OCSP Responder. Note that when used as a standalone OCSP Responder the marketing name of ADSS OCSP Server is used. When combined with other services such as signing, verification or other validation then ADSS Server is the product name normally used.

Overview

ADSS OCSP Server is an advanced x.509 certificate Validation Authority server that fully conforms to the IETF RFC 6960 standard. It is also FIPS 201 Certified (APL #1411) and approved for use by US federal agencies for HSPD-12 implementations.

It has been designed to operate as a robust validation hub solution capable of providing OCSP certificate validation services for multiple Certificate Authorities (CAs) concurrently. Simple or sophisticated validation policies are supported for each individual CA and ADSS OCSP Server provides a detailed historical record of all transactions together with an easy to use OCSP request and response viewer – essential for either billing and/or troubleshooting within managed service infrastructures or enterprise systems. It also includes easy to use security management, logging, reporting, role based access control and optional dual controls.

Key Features

▪ HTTP and HTTP/S interfaces to the OCSP protocol conforming to IETF RFC 6960
▪ Operates on behalf of one or more CAs with unique keys and policies per CA
▪ Designed for enterprise use, multi-third party use and national or global managed services
▪ Can be used with internal and external trust schemes to be minimise external traffic dependencies
▪ Provides sophisticated high availability facilities to ensure that the latest published CRL is monitored and quickly consumed to generate the appropriate OCSP responses.
▪ Provides a secure browser based management GUI that enforces role-based controls over operator actions including optional dual controls enabling secure remote management.
▪ Provides quick internal OCSP responses to the signature verification service for certificate status and long term signature generation according to ETSI and PDF standards.
▪ Provides detailed event and transaction logging and reporting to aid help desk queries, management reporting and auditing as well as legal and regulatory compliance.
▪ The OCSP service can be configured and managed along with digital signature creation, verification, certification and timestamp authority services using the same underlying technology and management interface on one or multiple servers.
▪ Supports the RSA PKCSv1.5 and PSS v2.1 padding schemes
▪ Supports multiple database technologies including:
  → Azure SQL Database (Database-as-a-service)
  → Oracle 12c, 11g
  → PostgreSQL v11.x, v10.x, v9.3.25
  → MySQL v8.x, v5.5.62 and Percona-XtraDB-Cluster 5.7.21
▪ Supports the options of using various HSMs for secure key management as well as smartcard based credentials for operator authentication.
▪ ADSS OCSP Server is designed to meet CWA 14167-1 and has been successfully assessed within a defence project environment.

Further Information References

This document is a quick guide to get a simple configuration of the OCSP Service installed, tested and operational. More detailed information is available in the following documents:
- ADSS Server Installation Guide – detailed installation guide
- ADSS Server Admin Manual – details all the administrative features
- ADSS Server SQL Server Installation Guide
- Ascertia has maintained an online knowledgebase for customer ease. You can follow these link for more details: [http://faqs.ascertia.com/display/AKBS/Ascertia+Knowledge+base](http://faqs.ascertia.com/display/AKBS/Ascertia+Knowledge+base)

### System Requirements

Please see the ADSS Server Installation Guide for supported operating systems, databases and other related information. You can also follow this online link: [https://www.ascertia.com/products/system-requirements/](https://www.ascertia.com/products/system-requirements/)

### Quick Installation and Configuration Steps

ADSS Server can be quickly installed for evaluation purposes using the following steps:

- Install MS SQL Server and create a new, empty database
- Install ADSS Server
- Generate the Keys and Certificates for the OCSP Service using the ADSS Key Manager
- Use the ADSS Trust Manager to add the CAs for which the OCSP Service will respond and then configure the polling of CRLs for these CAs
- Ensure CRL Monitor is running and CRLs are being automatically polled and downloaded. CRLs can also be manually imported into ADSS Server
- Configure the OCSP Service for the relevant CAs and policies
- Test the OCSP Service using Ascertia’s OCSP Client test tool
- Optionally monitor the OCSP Service using Ascertia’s OCSP Monitor product

The default installation configures ADSS Server to use its integral software crypto-libraries, however various hardware security modules (HSMs) can be supplied and used if required. For further information refer to the ADSS Server Admin Manual Key Manager. We recommended that you contact us for advice and guidance if you are configuring an HSM.

### Install MS SQL Server and create an ADSS Server database

Read the separate guide for installing and configuring MS SQL Server. The key points to note are:

- Ensure that mixed mode authentication is selected during the installation. Using Microsoft Windows Authentication will lead to installation issues.
- Ensure that TCP ports are set to 1433 (for IP1, IP2 and IP All)
- Configure a database owner with administrator permissions
  - **Note:** Ensure the language is set to English

### Install ADSS Server

- Extract the ADSS Server installation zip file to a target folder e.g. D:\ADSS-Server
  - **Note:** The folder path cannot have spaces so you cannot use “Program Files” or similar
- From <ADSS Server Installation Directory>/setup run install.bat which starts a configuration Wizard
  - **Note:** Setup cannot be run and completed more than once - If the evaluation needs to be re-installed then the ADSS Server installation directory needs to be deleted and the zip re-extracted.
- The ADSS Server Installation Wizard shows a welcome screen then the license agreement and then asks if you wish to upgrade an existing installation or if you are installing for the first time. For new users you are installing for the first time so select this option. If you are adding a second server you are also installing for the first time.
- Confirm the installation path and click Next >
- Select the license type i.e. one of the evaluation license options offered, or provide the path for the commercial license if you already have got one.
- Uncheck the option to use the sample data and configurations – these are not that useful for CRL Monitor.
- Select SQL Server and Typical Configurations and click Next >
- Enter the connection details for the ADSS evaluation database and click Next >
- Setup now attempts to connect to the database. If this fails, check the connection details are correct, if they are then the problem is often found to be either:
  → a) That the IP configurations are not enabled (use SQL Server Configuration Manager)
  → b) That SQL Server was not installed with mixed mode authentication (it will need to be re-installed)
- Select “Typical installation” and click Install
- After the progress bar completes leave the default Service Settings selected and click Finish
- The Windows installation wizard will appear so that the ADSS Server admin key and certificate can be installed in the browser. The certificate allows an administrator to securely login to the ADSS Admin Console over an SSL/TLS session with client and server authentication. Follow the wizard instructions and install the certificate in the Windows Personal store. The password of the Default Admin certificate is: password. This is an initial certificate and it should be replaced once ADSS Server is running.
- After this an HTML page opens in the default web browser providing a link to the ADSS Admin Console. Click on this link if using Internet Explorer. If using Firefox then you must browse to https://localhost:8774/adss/console to log into the ADSS Admin Console Firefox also wishes to see the keys and certificates in its local trust store.
  → The browser will indicate that the server certificate is not trusted – this is because a temporary certificate is used by ADSS Server at this time that can be changed later and trusted for production use. Select continue.
  → If you are presented with a list of client certificates - select the one called ADSS Default Admin
- At this point ADSS Server has been successfully installed and the ADSS Admin Console can now be used to configure the OCSP service.

**Configure the OCSP Service**

This quick guide deals with a simple configuration where the OCSP Service is configured as a standalone responder that responds for all certificates status requests. The relaying of status requests for certificates to other responders responsible for those certificates is explained further in the ADSS Administration Guide. Log into the ADSS Admin Console and follow these steps to configure the OCSP Service:

**Generate OCSP Response Signing key & Certificate:**

- Select the Key Manager top menu and then the Key Manager side menu
- Generate a new OCSP response signing key by clicking New, supplying the key alias information and a purpose as OCSP Response Signing from the Purpose drop down - Click OK
- Check the radio button for the key now identified by the key alias entered in the previous step and click Certificates.
- Key can be certified (Delegated/Self-Signed) by clicking the Create CSR/Certificates button, enter the certificate request details to be certified by Local CA, External CA or Self-signed.
  → Use Local CA option to certified the OCSP Response signing key from a configured local CA
  → Use External CA option to create a PKCS#10 for the OCSP Response signing key to be certified from an External CA. The certificate generated by the External CA can be imported into ADSS Server by clicking the Import button on the certificates screen. See the ADSS Server admin guide for more details.
  → Use Create Self-signed certificate option in order to create a self-signed OCSP certificate to authenticate the OCSP responses
**Note:** If you have an existing key to be used as OCS Response Signing then you can also import this existing key by using Import key button. Provide a key alias, certificate alias the path to the OCSP Response Signing PFX with the relevant password and select the purpose as OCSP Response Signing from the purpose drop down.

Some OCSP clients enforce the requirement for the OCSP response signature to be verified by a certificate issued by the **same** CA that issued the end entity (target) certificate whose status is being checked. This method must be used in these cases. An example is the Firefox OCSP client feature. Some clients also require the OCSP responder certificate to have an Extended Key Usage extension which is marked for “OCSP Signing”.

**Register CA(s) in Trust Manager:**
- Select the Trust Manager from the top menu
- Click the New button and “browse” to import the certificate of the CA. A CA friendly name is offered based on the certificate common name – use this or enter one of your choice.
- Check the registration purpose as CA (this will be used to verify other certificates and the signatures on downloaded CRLs), now click Next >
- On the Validation Policy screen select Local Cached CRL as the Primary Method and None as the Secondary Method and click Next >
- Add the URL of the CA’s CRL distribution point to the List of CRL Resources. Click on the resource in the list to highlight it and the click Test Connection. The CRL should be accessed and its signature should be verified OK.
- Check “Enable Automated Polling” and select “Start Polling at next CRL Update”
  → **Note:** These settings are dependent on the CAs CRL issuing policy - see the ADSS Admin Guide for more information on these settings.
- Click on the Next button and repeat until you reach on the Back-end Certificates page and click on the Finish button.
- Add another CA in the same way if required
- Go to the Server Manager tab and “Restart All Instances”
- Once restarted go to the CRL Monitor tab

**Download the Initial CRLs:**
- Within CRL Monitor click on CRL Details in the side menu
- Select a target CA and Click on View CRLs
- Click Auto Retrieve CRLs and the latest CRL for the target CRL should be downloaded and checked and trusted. All checks should finish with a green tick.
- Repeat this for all other configured CAs

**Add CA(s) in the OCSP Service and Configure Advance Settings:**
- Select the OCSP Service top menu and then the Registered CAs side menu
- Click the Add CA button and select the CA registered via the Trust Manager in the Register this CA for OCSP service drop down.
- Select, in the Client Communication Cert drop down, the correct OCSP Response Signing certificate that was created in Key Manager
  → **Note:** The remaining configurations in the Add CA screen has settings that are determined by the CA/OCSP responder policy - see the ADSS Admin Guide for more information.
- Click on the Insert button
- Click on the Advance Settings in the side menu, select the “Default OCSP Policy” tab. Now select the same ADSS OCSP Response Signing Certificate as before and click on the Update button. The Default Policy is used for all unsigned OCSP requests.
- Click on OCSP Service > Access Control to control access rights to the OCSP service if required based on SSL Client certificates, OCSP request signing certificates or IP addresses
Use Server Manager to Restart all ADSS Server Services:
- Go to the Server Manager tab and “Restart All Instances”

The ADSS OCSP Server system is now ready to process OCSP requests.

Testing the OCSP Service
- Download an evaluation version of the OCSP Client tool from the Ascertia web site
- Run OCSP Client tool, highlight any existing entries in the CertID window & click Remove
- Click Add. Browse for a Target Certificate that will be checked for its revocation status in an OCSP request. Browse for the Issuer Certificate for the Target Certificate.
  - Note: The Target Certificate would normally have been issued by the CA configured in the ADSS Server Trust Manager and the Issuer Certificate is the certificate of the CA registered in the ADSS Server Trust manager
- Click Add CertID/s
- From the top menu select File/Trust Anchors
- In the Add Trusted CAs field browse for an OCSP/CA Certificate that is the OCSP Response Signing certificate generated by the ADSS Server Key Manager. Click Trust It and then OK.
  - Note: The OCSP Response Signing certificate needs to be exported using the ADSS Server Key Manager to be available for import here. It allows the OCSP Client tool to verify the signature on an OCSP response.
- In the OCSP Responder Settings Field of the main dialog make the following settings: OCSP Responder Host = http://<machine name>, Port = 8777, Path = /adss/ocsp
  (Note: If the default Port and Path have been reconfigured then change these settings to match the OCSP Service)

Click the OCSP Client Send Request button and view the result details. Note that OCSP Client tool only allows 10 requests in evaluation mode!

Configuring the OCSP Service URL
The default paths and ports can be changed to suit further evaluation where OCSP clients make OCSP requests according to the URL provided in a certificate’s AIA (Authority Information Access) or where the OCSP client uses a pre-configured URL. The OCSP service can be accessed at these default URLs:
- **Plain HTTP:**
  - http://{server-name}:8777/adss/ocsp
  - http://{server-name}:8777
- **Server Authentication:**
  - https://{server-name}:8778/adss/ocsp
  - https://{server-name}:8778
- **Mutual Authentication:**
  - https://{server-name}:8779/adss/ocsp
  - https://{server-name}:8779

The default port can be changed to 80 for HTTP and 443 for HTTPS communications to achieve standard default port URLs i.e.:
- http://validation.ocsp.com
- https://validation.ocsp.com
Note:

→ The port numbers of 80 or 443 do not need to be specified. For more details on how to change the default ports follow this KB article:

http://faqs.ascertia.com/display/ADSS/Tomcat+Configurations#TomcatConfigurations-ChangingthedefaultportsforADSSServerservices

→ Alternatively, you can run a standard HTTP web server e.g. Microsoft IIS to redirect requests on port 80 or 443 to ADSS Server and in this case no change in ADSS port configurations is required. Follow this KB article to configure AJP Connector:

http://faqs.ascertia.com/pages/viewpage.action?pageId=1671317

### Troubleshooting ADSS Server

If problems arise when installing or running ADSS Server then please check the following:

- **Failed to connect to database when installing ADSS Server** – if ADSS Server setup wizard is unable to connect to the database then check that:
  → The database connection details are correct
  → The database server is up and running
  → The database user has sufficient access privileges

- **Failed to install ADSS Server using a new database** – if you are unable to install ADSS Server when using a new database then check that:
  → The database for ADSS Server has already been created
  → The same database has not been used for an earlier installation of ADSS Server
  → The database user has sufficient access privileges on the selected database

- **Unable to access ADSS Server console** – if ADSS Server console is not accessible after installation then check that:
  → The default client authentication certificate i.e. ADSS Default Admin is installed in Internet Explorer personal key store of the Windows desktop being used.
  → The appropriate default client authentication certificate i.e. ADSS Default Admin is being selected when accessing ADSS Server console.
  → The ADSS Server Windows service is started and is running
  → The database service is started and is running. Re-start ADSS Server Windows service if database server goes down while ADSS Server was running (especially if testing on XP).

- **Unable to process OCSP requests**
  → Check the ADSS Server Windows service is started and is running
  → Check that the ADSS OCSP service is running, by logging into the ADSS console and clicking on the OCSP Service Manager.
  → Check the URL and port number for the server and client

### Product Notes

1) The evaluation version of ADSS Server only allows up to 1000 OCSP transactions. The number of keys that can be generated and certified is limited to 20. The number of Trust Authorities and clients that can be registered is also restricted.

2) Ascertia can provide free phone based assistance, paid onsite assistance, training and additional services for ADSS Server.

### Contact Details

For Commercial Sales: +44 (0) 203 633 1177, sales@ascertia.com

For Technical Support: support@ascertia.com