



# Technical Bulletin #27

This technical bulletin describes how to configure an ACS Server that is outside a firewall, so that it can connect to a CMS Server that is behind the firewall.

**Note:** This technical bulletin applies to ACS version 4.6.2-23 or later.

---

## Issue

---

Users may have a configuration consisting of an ACS Server outside a firewall for access by various clients. For security reasons, the CMS Server may need to be inside the firewall. Without special configuration, the ACS Server would be unable to connect to the CMS Server.

---

## Before You Begin

---

This document assumes the following arrangement (machine/account names are up to you):

- A firewall for the domain:  
IP Address: 11.22.33.255
- An ACS server outside your firewall:  
Hostname: ACSHOST  
IP Address: 11.22.33.172
- An Astoria CMS server behind a firewall:  
Hostname: DOMAIN\CMSHOST  
IP Address: 192.168.0.204
- A Windows userID on the ACSHOST:  
UserName: ACSHOST\acsAdmin
- A Windows userID on the CMSHOST:  
UserName: CMSHOST\acsAdmin
- An Astoria database user created with the Astoria Database Administration Tool:  
UserName: acsAdmin

**Note:** ACSHOST and CMSHOST UserNames must be identical. In addition, verify that you have a license file for running ACS on ACSHOST and CMS on CMSHOST.

---

## Resolution

---

The following areas must be configured and installed as described.

### Configure the Firewall

---

Configure your firewall(s) to permit TCP traffic on these ports going from the ACSHOST to the CMSHOST:

Table 1: Ports for Firewall (ACS to CMS)

Port	From	To	Description
7852/TCP	ACSHOST	CMSHOST	Client > Astoria Server
7854/TCP	ACSHOST	CMSHOST	Client > Astoria License Server
7859/TCP	ACSHOST	CMSHOST	Client > Astoria Server (Search)
51025/TCP	ACSHOST	CMSHOST	Client > ObjectStore server
51041/TCP	ACSHOST	CMSHOST	Client > OStore Cache Manager

Configure your firewall(s) to permit TCP traffic on these ports going from the CMSHOST to the ACSHOST:

Table 2: Ports for Firewall (CMS to ACS)

Port	From	To	Description
51031/TCP	CMSHOST	ACSHOST	ObjectStore Server > OStore Cache Manager
51050/TCP	CMSHOST	ACSHOST	OStore Cache Manager notification

**Note:** Your ACSHOST and CMSHOST machines may be running Microsoft Windows Firewall or a third-party software firewall, or they may not have any firewall software enabled. There may be one or more firewalls in between the ACSHOST, CMSHOST, and browser machines. All firewalls must be configured to support the TCP traffic as described above. It is beyond the scope of this technical bulletin to describe specific firewall software or network configurations.

In addition, ACS requires access to an SMTP server to generate emails for notifications. If the ACSHOST is outside the firewall, it requires access to an SMTP server that is either a) also outside the firewall, or b) inside the firewall with port 25 available from the ACSHOST through the firewall to the SMTP server.

### Configure Connectivity

---

The two machines must know each other by hostname. The method described here hardwires the IP addresses, but IP addresses can change. Consult your administrator for guidance.

- Verify that CMSHOST knows ACSHOST by hostname.

On CMSHOST, edit `<windows>\system32\drivers\etc\hosts`, and include:

```
; example - use actual ACS hostname and IP address
11.22.33.172      ACSHOST
```

- Verify that ACSHOST knows CMSHOST by hostname.

On ACSHOST, edit `<windows>\system32\drivers\etc\hosts`, and include:

```
; example - use actual CMS hostname and firewall IP address
11.22.33.255     CMSHOST
```

## Configure User Accounts

---

User accounts must be created.

- On ACSHOST, create a local Windows user account for ACS Services to use.

For example, the user account is ACSHOST\acsAdmin, and the password is "acspass".

Verify that acsAdmin is an administrator and has the proper privileges (Act as part of the OS, Log on as a batch job, and Log on as a service).

- On CMSHOST, create a corresponding Windows user account (e.g. acsAdmin).

Specify the same password (e.g., "acspass").

**Note:** The acsAdmin account on CMSHOST does not require any special privileges.

- On ACSHOST, set the following system environment variable:

```
OS_AUTH=NP
```

## Install Astoria Client

---

**To install the Astoria Client onto the ACSHost machine:**

- 1 Log off ACSHOST and log into your Windows desktop as ACSHOST\acsAdmin.
- 2 Install the Astoria Client.
- 3 Confirm you can open the database using the Astoria client applications on ACSHOST:

Run **nvnavig.exe**, on ACSHOST.

When prompted for credentials, supply Windows credentials that are valid on CMSHOST:

```
UserName: acsAdmin
```

```
Password: acspass
```

## Install ACS

---

**To install ACS onto the ACSHost machine:**

- 1 Login to the ACSHOST Windows desktop as user ACSHOST\acsAdmin.

## 2 Run Phase1 Setup.

At "Please specify a valid userID and password", specify CMSHOST credentials:

UserName: acsAdmin

Password: acspass

At "Please enter the credentials to run Web Services", specify ACSHOST credentials:

UserName: acsAdmin

Domain: ACSHOST

Password: acspass

## 3 If prompted to reboot upon Phase 1 Setup completion, do so before continuing.

## 4 Encrypt the credentials that ACS services should use to open the database.

Copy the python script **encPassword.py** from the Extras directory on your install media (version 4.6.2-23 or later) to your astoria\jython directory.

In a command shell, using your actual astoria directory path, enter the following:

```
SET LSPEED_CLASSPATH=c:\astoria\bin\xdmisc.jar
cd /d c:\astoria\jython
CALL jython.bat encPassword.py
```

When prompted, enter the plaintext password for the CMSHOST acsAdmin account (e.g. acspass). **Note:** It will echo an encrypted password (e.g. "YadaYadaYada==").

Copy the encrypted password to your Clipboard.

## 5 Specify the credentials that ACS Services should use to open the database

Edit **c:\program files\astoria software\common.cfg** by pasting the encrypted password entries as shown here:

```
[com.lspeed.astoria.SessionController]
UserName = AstoriaAdmin
EncryptedPassword = YadaYadaYada==

[com.lspeed.astoria.DatabaseController]
UserName = AstoriaAdmin
EncryptedPassword = YadaYadaYada==
```

## 6 Run Phase2 Setup

## 7 When Phase2 completes, use your browser to visit **http://ACSHOST/ief**

**Note:** Whenever you are prompted by a browser login, use the ACSHOST credentials (acsAdmin / acspass).

Click on the Web Services URL. After logging in, you should see a simple table containing some cryptic information.

Click the Back button, and click on WebDAV. You should see "Astoria WebDAV Server".

Click the Back button and click on the WebAccess URL (the first URL). After logging in, you should see the Web Access application that you installed.

## 8 Delete the file **encPassword.py** from your machine.