ATHEX Gateway

ATHEX Gateway Server

Systems and Network Preparation Instructions

Version 3.0.1

A T H E N S
EXCHANGE S.A.

Technological Systems & Services Directorate

Revision List

Version	Date	Description
2.0.0.1	06/12/2016	• Added support for Windows 2012 Server R2.
3.0.0	07/12/2017	• Updated section 4 “Network Time Protocol Client Setup” • Updated list of supported OSes on section 2.1
3.0.1	05/02/2018	• Corrected IP of NTP server.

Contents

1 Introduction

This document contains a set of instructions for the installation and parameterization of the Operating System and the networking environment of the production or shadow ATHEX Gateway server, operating either in primary or backup mode (referred as *GATEWAY* below for simplicity). The *GATEWAY* will be located in the ATHEX Member's site and will remain under ATHEX member's management responsibility.

ATHEX Gateway application consists of two software modules implementing two different communication interfaces:

- ODL Service application implementing ODL API interface
- ASE Service application implementing FIX protocol interface

Generally, ODL API uses the Microsoft Windows Security architecture for controlling and checking access permissions; hence a **Domain Controller** is needed. During the installation procedure users and groups will be created to the local Microsoft Windows Domain and the *GATEWAY* will need to join that Domain. However, if it is absolutely necessary, it can also operate without the use of a Domain Controller. For this arrangement, the required modifications in the operating system installation and configuration procedure are described in Chapter 7: Appendix B: Using ODL Gateway without a Domain Controller.

One **INSTALLATION FORM** containing all the installation parameters needed, accompanies this document. This form must be available to the person responsible to install the environment. When the notation **Text** is used in the present document, that person should find and fill the correct value from the **INSTALLATION FORM**.

2 Operating System Installation and Configuration

This chapter describes the required configuration of the operating system.

2.1 Installation

A full installation of one of the following operating systems should be performed on the system *GATEWAY* in Logical Drive 1 (Drive Letter C:), by selecting the default settings during the non-graphical installation part:

- MS Windows Server 2008 R2
- MS Windows Server 2012 R2
- MS Windows Server 2016

After completion of the Operating System installation, the actions described in the following paragraphs must be done using the built-in **Administrator** account.

2.2 General Settings

- The built-in user account **Administrator** should have full system privileges.
- The installation of the network card drivers should be done by following the instructions on the corresponding installation technical manuals. Upon completion of the drivers' installation, you should test their correct functionality by using the software provided by the vendor.
- The recommended system's time format (long time format in Windows Server 2008 R2 or later) is **HH:mm:ss**.

2.3 ATHEXnet-NIC Network Settings

The network speed will be defined at 100 Mbps Media Type 100BASE-TX (100 MBPS)] full duplex [Duplex = Full Duplex]. You should reboot the computer after the above settings and test the card's correct operation using the utility provided by the NIC manufacturer.

- TCP/IP should be the only installed communication protocol on GATEWAY. The settings of the TCP/IP stack on each server are categorised as either common or specific to the ATHEX Members. The specific settings, depending on the type (Production or Shadow) and the operating mode (primary or backup) of the GATEWAY, of ATHEXnet-NIC for the installation are:
  - **Production** GATEWAY operating in **primary mode**

ATHEXnet-NIC	
IP – Address	**ETSGW_ASE_IP**
Default Gateway	The first 3 bytes are identical to the <IP – Address> above and the last one must be set to **65** (e.g. a.b.c.**65)**

  - Production GATEWAY operating in **backup mode**

ATHEXnet-NIC	
IP – Address	**ETSGW_ASE_IP_BACKUP**
Default Gateway	The first 3 bytes are identical to the <IP – Address> above and the last one must be set to **65** (e.g. a.b.c.**65)**

- Shadow GATEWAY operating in **primary mode**

ATHEXnet-NIC	
IP – Address	**ETSSGW_ASE_IP**
Default Gateway	The first 3 bytes are identical to the <IP – Address> above and the last one must be set to **65** (e.g. a.b.c.**65)**

- **Shadow** GATEWAY operating in **backup mode**

ATHEXnet-NIC	
IP – Address	**ETSSGW_ASE_IP_BACKUP**
Default Gateway	The first 3 bytes are identical to the <IP – Address> above and the last one must be set to **65** (e.g. a.b.c.**65)**

- The common settings of the ATHEXnet-N10IC for all ATHEX Members and GATEWAYS regarding the Subnet mask are as follows:

ATHEXnet-NIC	
Subnet Mask	255.255.255.192

- The common settings of the ATHEXnet-NIC for all ATHEX Members and GATEWAYS regarding the ATHEX DNS servers are as follows:

ATHEXnet-NIC		
Primary DNS Server	**IP Address**	10.200.131.17
Secondary DNS Server	**IP Address**	10.200.131.18

2.4 ATHEX Member-net-NIC Settings

- The NIC used to connect *GATEWAY* to the internal ATHEX Member's network should be configured according to the ATHEX Member network characteristics.

- TCP/IP should be the only installed communication protocol on the GATEWAY. The TCP/IP settings will be configured by ATHEX Member's technical staff that following the company's IP addressing scheme in the Private Internet Address Space (i.e., no use of Official Public Internet IP Addresses).

2.5 Oracle Client Installation

In order for the GATEWAY to connect to the XNET Server or the DSS Server, the Oracle Client 11g release 2 (Windows 32-bit) or later must be installed.

At the time of writing of this document the latest **Oracle Client (Windows 32-bit)** release is 11.2.0.1.0. (Oracle Database 11*g* Release 2 Client (11.2.0.1.0) for Microsoft Windows (32-bit))

During installation make sure you select the **Administrator** installation type.

2.6 Security Settings

Depending on the interfaces (FIX, ODL API or Both) used by member, the following security settings must be applied:

2.6.1 On the Domain Controller

ODL API or Both

The following accounts and user groups should be created on the Domain Controller that *GATEWAY* would join, located at the Member's LAN (DMZ):

User Groups:

- A Global Users Group "**ETS_Brokers**"
- A Global Users Group "**ETS_Admins**"

Domain Accounts:

- **ETS_ADMIN1** as a member of "**Users**" and "**ETS_Admins**"
- **ETS_BROKER1** as a member of "**Users**" and "**ETS_Brokers**"
- **ETS_BROKER2** as a member of "**Users**" and "**ETS_Brokers**"

Note:

ETS_BROKER2 account may not be needed. It will be used only if a second application wants to access the gateway. If more applications are used, then more accounts (ets_broker3 etc.) must be created. For all the above accounts please set appropriate passwords and keep them safely.

- **ETS_SERVICE** as a member of "**Users**"

The account **ETS_SERVICE** should have the following characteristics:

- The password should never expire (Password Never Expires)
- The password should never be changed by the user (User Cannot Change Password)
- The user will not change the password at next logon ("User must change password at next logon" unchecked).

FIX Protocol only

No users or groups needed on Domain Controller for FIX Protocol.

2.6.2 On the GATEWAY

ODL API or Both

Before creating the User Groups below, the system *GATEWAY* should have joined the Domain in the Member's LAN. The groups that must be created are:

- A Local Users Group **"ETS_Brokers"** with member the already created Global Users Group **"ETS_Brokers"** in the Member's domain
- A Local Users Group **"ETS_Admins"** with member the already created Global Users Group **"ETS_Admins"** in the Member's domain.

If ***FIX Protocol*** Interface is used the users bellow must be created:

- A Local User **"ASE_Service"** that belongs in **"ETS_Brokers"** and **"ETS_Admins"** local groups.
- A Local User **"ETS_Service" (only if ODL interface is not used)**.

Local Security Policy

On the GATEWAY some modifications to the local policies have to be made.

1. Click on Start, Administrative Tools and then choose Local Security Policy.
2. In the console tree, click Local Policies and then click User Rights Assignment.

Policy	Security Setting
Allow Log on locally.	Only <Computer name>\Administrators
Access this computer from network	Only <Computer name>\Administrators, ETS_Admins, ETS_Brokers , ETS_Service
Log on as a Service	Add ETS_Service and ASE_Service
Shut down the system.	Only <Computer name>\Administrators

3. In the console tree, click Local Policies and then click Audit Policy.

Policy	Security Setting
Audit logon event	Success, Failure
Audit privilege use	Success, Failure
Audit policy change	Success, Failure
Audit system events	Success, Failure

Event Viewer

1. Click on Start, Administrative Tools and then choose Event Viewer.
2. In the console tree, click Windows Logs.
3. Right-click Application and then choose Properties
4. Make sure that:
    a. Maximum log size is **at least** 16384KB
    b. Overwrite event as needed is selected.
5. Follow steps 3 and 4 for Security and System logs.

2.6.3 On each Client

Local Security Policy

1. Click on Start, Administrative Tools and then choose Local Security Policy.
2. In the console tree, click Local Policies and then click Security Settings.
3. Make sure that Network access: Sharing and security model… is set to Classic.

3 Network Time Protocol Client Setup

The *GATEWAY* must synchronize its clock with ATHEX NTP servers and consequently with OASIS/ETS. An NTP client must be installed and configured as follows to achieve the synchronization with the ATHEX NTP servers over the ATHEXnet:

- Log on to the Windows Server system using the domain administrator account.
- Right-click on the **Command Prompt** icon and select **Run as administrator**.
- Enter the following commands:
  - `net stop w32time`
  - `w32tm /config /syncfromflags:manual /manualpeerlist:"10.200.1.2","10.200.2.2"`
  - `net start w32time`
- Run ***regedit.***
- Select the key *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpClient*
- In the right pane, right-click **SpecialPollInterval**, and then click Modify.
- In Edit DWORD Value, type 900 (decimal) in the Value data box, and then click OK.
- Make sure that the "Windows Time" service is set to **startup** automatically.

For confirmation of setting the ATHEX NTP servers execute the following command:

- `w32tm /query /configuration`

Note*:*

In order to achieve synchronization of the ATHEX Clients with ATHEX NTP servers it is recommended to configure GATEWAY as an NTP Server. The NTP Server configuration steps are the following:

- Run ***regedit.***
- Select the key *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpServer*
- In the right pane, right-click **Enabled**, and then click Modify.
- In Edit DWORD Value, type 1 in the Value data box, and then click OK.
- Right-click on the **Command Prompt** icon and select **Run as administrator**.
- Enter the following command:
  - `net stop w32time && net start w32time`

Finally, each machine running an ODL Client must be configured to use the ATHEX Gateway as its NTP server.

4 Network Connection Testing

To test the network connectivity the ATHEX Member technical staff should:

- Issue a Ping command to the IP Address (127.0.0.1) of the system's Loopback Interface. The reply response should be less or equal to 10ms.
- Issue a Ping command to the IP Addresses of the system's Ethernet Interface (DMZ-NIC). The reply response should be less or equal to 10ms.
- Issue a Ping command to the system's Default Gateway. The reply response should be less or equal to 10ms.

5 Technical Support

For any questions or technical support needs concerning the ATHEX Gateway Installation the ATHEX Member technical staff should contact:

Members Support Department
Tel: (+30) 210 - 33.66.393
Tel: (+30) 210 - 33.66.385
Fax: (+30) 210 - 33.66.286
E-mail: Members-Support@helex.gr

6 Appendix A: Firewall configuration guidelines

If the ATHEX Member decides to setup a firewall between the *GATEWAY* and the ATHEX infrastructure then the following data flows should be considered:

Protocol	**Source IP Address**	**Source port**	**Destination IP Address**	**Destination port**
Application Traffic				
ODL traffic with Production COM cluster				
Primary production ODL Gateway				
tcp	**ETSGW_ASE_IP**	**LocalControlPortNumber_pro**	10.200.121.19	**RemoteControlPortNumber_pro**
tcp	10.200.121.17	gt 1023	**ETSGW_ASE_IP**	**LocalDataPortNumber_pro**
tcp	10.200.121.18	gt 1023	**ETSGW_ASE_IP**	**LocalDataPortNumber_pro**
Secondary production ODL Gateway				
tcp	**ETSGW_ASE_IP_BACKUP**	**LocalControlPortNumber_pro**	10.200.121.19	**RemoteControlPortNumber_pro**
tcp	10.200.121.17	gt 1023	**ETSGW_ASE_IP_BACKUP**	**LocalDataPortNumber_pro**
tcp	10.200.121.18	gt 1023	**ETSGW_ASE_IP_BACKUP**	**LocalDataPortNumber_pro**
ODL traffic with Shadow COM cluster				
Primary production ODL Gateway				
tcp	**ETSGW_ASE_IP**	**LocalControlPortNumber_pro**	10.200.121.51	**RemoteControlPortNumber_pro**
tcp	10.200.121.49	gt 1023	**ETSGW_ASE_IP**	**LocalDataPortNumber_pro**
tcp	10.200.121.50	gt 1023	**ETSGW_ASE_IP**	**LocalDataPortNumber_pro**
Secondary production ODL Gateway				
tcp	**ETSGW_ASE_IP_BACKUP**	**LocalControlPortNumber_pro**	10.200.121.51	**RemoteControlPortNumber_pro**
tcp	10.200.121.49	gt 1023	**ETSGW_ASE_IP_BACKUP**	**LocalDataPortNumber_pro**
tcp	10.200.121.50	gt 1023	**ETSGW_ASE_IP_BACKUP**	**LocalDataPortNumber_pro**
Primary shadow ODL Gateway				
tcp	**ETSSGW_ASE_IP**	**LocalControlPortNumber_pro**	10.200.121.51	**RemoteControlPortNumber_pro**
tcp	10.200.121.49	gt 1023	**ETSSGW_ASE_IP**	**LocalDataPortNumber_pro**
tcp	10.200.121.50	gt 1023	**ETSSGW_ASE_IP**	**LocalDataPortNumber_pro**
Secondary shadow ODL Gateway				
tcp	**ETSSGW_ASE_IP_BACKUP**	**LocalControlPortNumber_pro**	10.200.121.51	**RemoteControlPortNumber_pro**
tcp	10.200.121.49	gt 1023	**ETSSGW_ASE_IP_BACKUP**	**LocalDataPortNumber_pro**
tcp	10.200.121.50	gt 1023	**ETSSGW_ASE_IP_BACKUP**	**LocalDataPortNumber_pro**
ODL traffic with Development COM				
Primary shadow ODL Gateway				
tcp	**ETSSGW_ASE_IP**	**LocalControlPortNumber**	10.200.121.34	**RemoteControlPortNumber**
tcp	10.200.121.34	gt 1023	**ETSSGW_ASE_IP**	**LocalDataPortNumber**
Secondary shadow ODL Gateway				
tcp	**ETSSGW_ASE_IP_BACKUP**	**LocalControlPortNumber**	10.200.121.34	**RemoteControlPortNumber**
tcp	10.200.121.34	gt 1023	**ETSSGW_ASE_IP_BACKUP**	**LocalDataPortNumber**
Other Traffic				
DNS traffic				
udp	**ETSGW_ASE_IP**	gt 1023	10.200.131.17	Domain
udp	**ETSGW_ASE_IP**	gt 1023	10.200.131.18	domain

udp	**ETSGW_ASE_IP_BACKUP**	gt 1023	10.200.131.17	domain
udp	**ETSGW_ASE_IP_BACKUP**	gt 1023	10.200.131.18	domain
udp	**ETSSGW_ASE_IP**	gt 1023	10.200.131.17	domain
udp	**ETSSGW_ASE_IP**	gt 1023	10.200.131.18	domain
udp	**ETSSGW_ASE_IP_BACKUP**	gt 1023	10.200.131.17	domain
udp	**ETSSGW_ASE_IP_BACKUP**	gt 1023	10.200.131.18	domain
NTP traffic				
udp	**ETSGW_ASE_IP**	gt 1023	10.200.121.41	ntp
udp	**ETSGW_ASE_IP**	gt 1023	10.200.121.141	ntp
udp	**ETSGW_ASE_IP_BACKUP**	gt 1023	10.200.121.41	ntp
udp	**ETSGW_ASE_IP_BACKUP**	gt 1023	10.200.121.141	ntp
udp	**ETSSGW_ASE_IP**	gt 1023	10.200.121.41	ntp
udp	**ETSSGW_ASE_IP**	gt 1023	10.200.121.141	ntp
udp	**ETSSGW_ASE_IP_BACKUP**	gt 1023	10.200.121.41	ntp
udp	**ETSSGW_ASE_IP_BACKUP**	gt 1023	10.200.121.141	ntp
FTP – Secure FTP traffic				
tcp	**ETSGW_ASE_IP**	gt 1023	10.200.131.33	20 - 22
tcp	**ETSGW_ASE_IP_BACKUP**	gt 1023	10.200.131.33	20 - 22
tcp	**ETSSGW_ASE_IP**	gt 1023	10.200.131.33	20 - 22
tcp	**ETSSGW_ASE_IP_BACKUP**	gt 1023	10.200.131.33	20 - 22

Apparently, in the case of an ATHEX Member that needs to install a set of GATEWAYs other than the full four (e.g. Primary production GATEWAY and Primary shadow GATEWAY), only the relevant firewall flows must be allowed.

For any questions regarding this firewall configuration the ATHEX Member technical staff should contact NOC@helex.gr

7 Appendix B: Using ODL Gateway without a Domain Controller

In order to run the ODL Gateway without using a Domain Controller, **all user accounts** (ETS_service, ETS_Broker1, …, ETS_Admin1, …) **shall be locally created both in the ODL Gateway and in the ODL Client(s)** that will be connected to the ODL Gateway. These local user accounts shall be **identical** (username, password, access rights) in all machines (Gateway and Clients).

7.1 Parameterization of the ODL Gateway

The steps that shall be followed during the parameterization of the Operating System and the networking environment of the production or shadow ODL Gateway server, operating either in primary or backup mode are:

1. Creation of the **ETS_Service** local account running the "ODL Gateway" service
   a. Create a local user account:
      Username: ETS_Service
      Password: <ETS_Service_password>
      Password never expires: True
      Member of: Users, Power Users
   b. Add this account to the list: **Local Security Policy -> Security Settings -> Local Policies -> User Rights Assignment -> Log on as a service**

2. Creation of the **ETS_Admins** and the **ETS_Brokers** local user groups
   a. Create the local user group ETS_Brokers
   b. Create the local user group ETS_Admins
   c. Add these groups to the list: **Local Security Policy -> Security Settings -> Local Policies -> User Rights Assignment -> Access this computer from the network**

   Note: The ETS_Brokers local user group shall contain the local users ETS_Broker1, …and the ETS_Admins local user group shall contain the local users ETS_Admin1, …

3. Creation of the **ETS_Broker1, …, ETS_Admin1, …** local accounts
   a. Create the local user account **ETS_Broker1**:
      Username: ETS_Broker1
      Password: <ETS_Broker1_password>
      Password never expires: True
      Member of: ETS_Brokers, Users

   ……
   b. Create the local user account **ETS_Admin1**:
      Username: ETS_Admin1
      Password: <ETS_Admin1_password>
      Password never expires: True
      Member of: ETS_Admins, Users

   …….

Note: The Domain users (ETS_Admin1, …, ETS_Broker1, …, ETS_Service) as well as the Global User Groups are not needed under this scheme.

7.2 Parameterization of the ODL Clients

In the ODL Clients, the following local user accounts must be created:

- ETS_Service
- ETS_Broker1, ...
- ETS_Admin1, ...

No user groups shall be created.

The steps that shall be followed during the parameterization of the Operating System in the ODL clients are:

1. Creation of the **ETS_Service** local account **identical** (same user name and password) to the one created in the ODL Gateway
   a. Create a local user account:
      Username: ETS_Service
      Password: <ETS_Service_password>
      Password never expires: True
      Member of: Users

2. Creation of the **ETS_Broker1, …, ETS_Admin1, …** local accounts **identical** (same username and password) to those created in the ODL Gateway
   a. Create the local user account **ETS_Broker1**:
      Username: ETS_Broker1
      Password: <ETS_Broker1_password>
      Password never expires: True
      Member of: Users

   ……
   b. Create the local user account **ETS_Admin1**:
      Username: ETS_Admin1
      Password: <ETS_Admin1_password>
      Password never expires: True
      Member of: Users

   …….