EntireX Security under z/VSE

This chapter introduces EntireX Security under z/VSE through overviews of the functionality and components of EntireX Security. The location where Broker Kernel is installed determines the functionality made available for EntireX Security. This chapter covers the following topics:

- Introduction
- EntireX Security for EntireX Broker
- Configuration Options for Broker

Note:
Installation of the security software is described under *Installing EntireX Security under z/VSE*.

Introduction

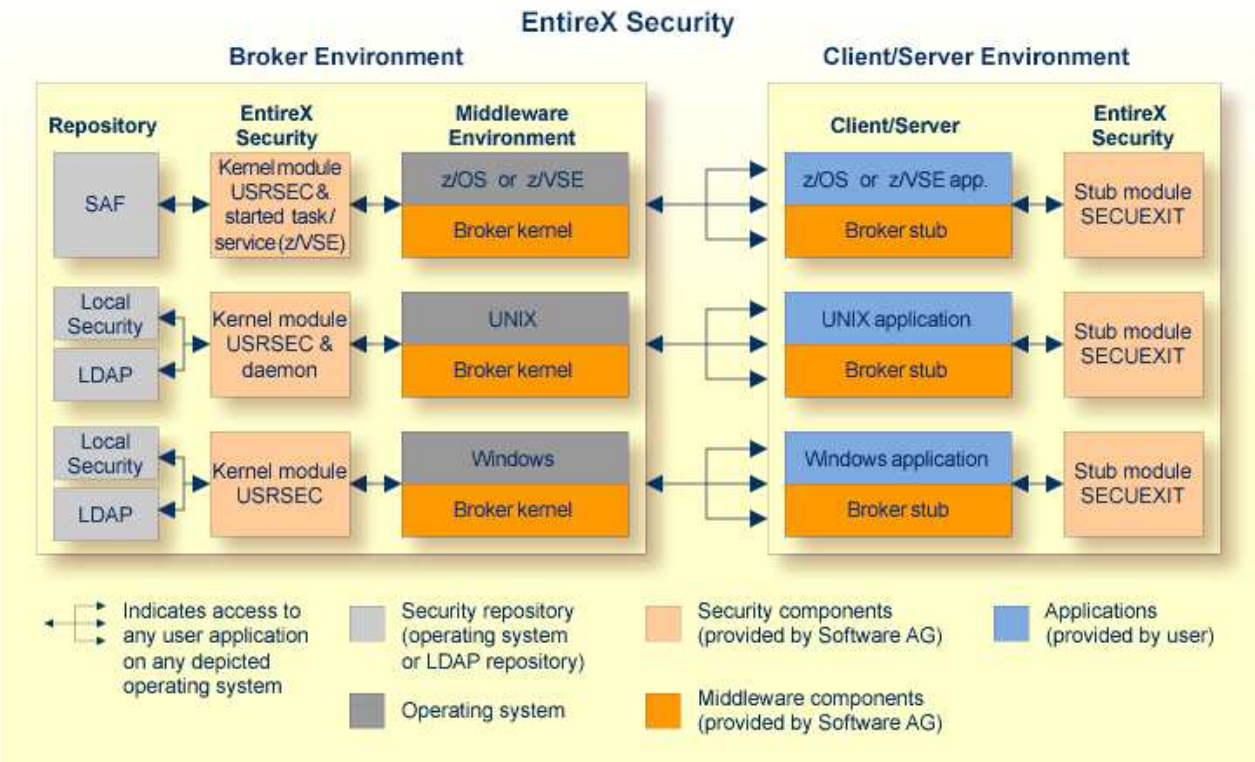
Functionality of EntireX Security

This table lists the security functionality available with EntireX Security running Broker Kernel under the respective operating system. See also *Configuration Options for Broker*.

Security Functionality	z/OS	UNIX	Windows	BS2000/OSD	z/VSE	Comment
Authentication of user	Yes	Yes	Yes	Yes	Yes	Verify User ID password.
User password change	Yes	No	No	No	No	
LDAP authentication	No	Yes	Yes	No	No	Authenticate using LDAP repository.
Trusted user ID	Yes	No	No	No	No	Trusted computer base, avoiding plain text password.
Verified client user ID	Yes	No	No	Yes	Yes	Provide verified identity of client to server.
Authorization of client request	Yes	No	No	No	No	
Authorization of server register	Yes	No	No	No	No	
Authorize IP connection	Yes	No	No	No	No	
Authorization rules	No	Yes	Yes	No	No	Check rules stored in an LDAP repository. These rules are maintained using an agent of System Management Hub, and are independent of the LDAP authentication mechanism. **Note:** These rules can be stored either in the same or a different LDAP repository.
Encryption of application data	Yes	Yes	Yes	No	Yes	RC4-compatible algorithm.
Guaranteed encryption	Yes	Yes	Yes	No	Yes	Allows administrator to require encryption for specific services.
SSL	Yes	Yes	Yes	No	No	Industry standard encryption mechanism.

EntireX Security Components

This diagram depicts the location where the Broker kernel must be installed and where the Broker stubs can be installed. It also depicts the location of the security components of the kernel and stubs of Broker.



EntireX Security for EntireX Broker

EntireX Broker acts as an agent to make the creation and operation of client/server applications simpler and more effective. Any number of server applications can be built for use by any number of clients. EntireX Security allows you to protect your server applications and clients independently.

Clients and servers are authenticated by user ID and password on their first contact with the system.

Configuration Options for Broker

This section describes the parameters for configuring EntireX Security under z/VSE. You may either accept or modify the default settings which are specified in the Broker attribute file `DEFAULTS=SECURITY`. See also *Security-specific Attributes* under *Broker Attributes* and *Operator Commands*.

This section covers the following topics:

- Authentication
- Guaranteed Encryption / Decryption Mechanism
- Password to Uppercase
- Security Level

Authentication

Authentication is mandatory and performed for both client and server applications based on user ID and password. First contact with the Broker results in the host security system being referenced. If authentication fails, access is denied and the application is informed with a suitable error message.

It is the responsibility of both client and server applications to supply a valid user ID and password when calling the Broker. The user ID must be supplied with all commands. The password is required only for the first command and should not be supplied subsequently, except when executing multiple instances of the same application.

Authentication expires after a period of non-activity after which it must be repeated. User ID and password must be resupplied before further access is possible. The time limits `CLIENT-NONACT` and `SERVER-NONACT` determine these timeout periods and are defined in the Broker attribute file.

Guaranteed Encryption / Decryption Mechanism

EntireX Security ensures message encryption consistency regardless of any configuration errors. This means that if the relevant assembly parameters or environment variables are incorrectly or inconsistently specified, the integrity of the Broker message is honored. This feature requires upgrade of all EntireX Security Broker stub and kernel components in all places.

See Broker attribute `ENCRYPTION-LEVEL` and control block field `ENCRYPTION-LEVEL`.

Password to Uppercase

To cater for situations where a site is in transition from uppercase to mixed case passwords setting this parameter can convert all passwords to uppercase. It is not recommended you use this option by default.

`PASSWORD-TO-UPPER-CASE={NO,YES}`	Convert password to uppercase.

Security Level

By default, EntireX Security furnishes authentication with optional encryption of send/receive buffers. The following parameter can be used to modify the functionality of EntireX Security:

`SECURITY-LEVEL=ENCRYPTION`	No authentication or authorization checks performed. The only functionality available in this mode is message privacy.
`SECURITY-LEVEL=AUTHENTICATION`	User authentication is performed but without any resource authorization (the normal default operation).