

EntireX Security under UNIX

This chapter introduces EntireX Security under UNIX 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:

- Functionality of EntireX Security
- EntireX Security Components

Note:

Setting up EntireX Security is described under *Setting up EntireX Security under UNIX*.

Functionality of EntireX Security

This table lists the security functionality available with EntireX Security running Broker Kernel under z/OS, UNIX or Windows.

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.

