Kerio Connect

Distributed domain

This manual provides description on the distributed domain in Kerio Connect version *8.3*. All additional modifications and updates reserved.

For current versions of the product and related manuals, check http://www.kerio.com/support/kerio-connect.

Contents

Chapter 1
Distributed domain

If your company uses more Kerio Connect servers physically scattered (located in different cities, countries, continents), you can now connect them together and move all users across all servers involved into a single email domain (distributed domain).

For proper functionality of the distributed domain, it is necessary that users are mapped from a directory service.

After the distributed domain is configured, the users will be able:

- to be members of common user groups,

- to access shared contacts (Global Address List),

- to reserve common resources,

- to plan meetings for all users in the distributed domain.

Distributed domain does not support:

- load balancing,

- folder sharing (including public folders),

- sharing of local users and user groups (users and groups that are not mapped from the directory service).

The setting and administration of distributed domains is only possible through Kerio Connect Administration.

Chapter 2
System requirements

Hardware configuration of computers on which servers involved in the distributed domain are installed is identical with the configuration used for any Kerio Connect installation.

It is only necessary to keep in mind that (both incoming and outgoing) traffic is processed through the master server and adapt the master server system requirements to the total number of users in the entire distributed domain.

Licensing policy

To add servers to the distributed domain, you will need a separate license for the corresponding number of users installed on each server.

Number of users is counted by email mailboxes/accounts created in the Kerio Connect or imported from the domain. Number of mailing lists, resources, aliases and domains is not limited.

In case of users mapped from the LDAP database of the directory service, all users created in this database are counted as individual licenses (all active users).

Once the number of licensed users is exceeded no other users will be allowed to connect to their accounts.

If you attempt to migrate users to a server where the number of licensed users has already been reached, Kerio Connect will deny the migration.

Chapter 4
How it works

To describe the function of distributed domain, it is necessary to separate the user accounts setting from mail delivery, resource sharing and Free/Busy server.

4.1 Master/Slave topology

The *Kerio Connect's* distributed domain works on the master/slave basis.

Master server

One of the servers (e.g. in the company headquarters) is set as the master server. To be added to the distributed domain, other servers must connect to the master server.

Master server:

- is the central (input and output) point of the distributed domain,

- receives mail and forwards it to the addressee's home server,

- sends mail received from slave servers,

- has an MX record set for the entire domain,

- provides antivirus and antispam check of the delivered mail.

For master server, it is recommended to use Kerio Connect with the integrated Sophos antivirus engine.

For correct communication of the master server with its slave servers, it is necessary to allow bi-directional traffic on the following ports:

- 587, 80, 44337 (TCP and UDP).

> *Warning:*
> To enable periodic archiving of traffic in the distributed domain, the mail must be both sent and received through a single central server (master server).
> It is therefore recommended to set the master server as the relay SMTP server for outgoing email on every slave server.

> *Warning:*
> To make the traffic as secure as possible, it is recommended to interconnect all servers in the distributed domain via a VPN (Virtual Private Network).

Slave server

Any other servers connected to the distributed domain are so called slave servers.

For correct communication between slave servers, it is necessary to allow bi-directional traffic on the following ports:

- 587 and 80.

> *Warning:*
> Upon connection, slave servers inherit all domain settings of the distributed domain (including settings of shared folders) from the master server.

4.2 User accounts and their setting

Every server in the distributed domain (either slave or the master) is connected directly to the server with a directory service. Any changes made in the directory service take effect on all the servers in the distributed domain (see figure 4.1).
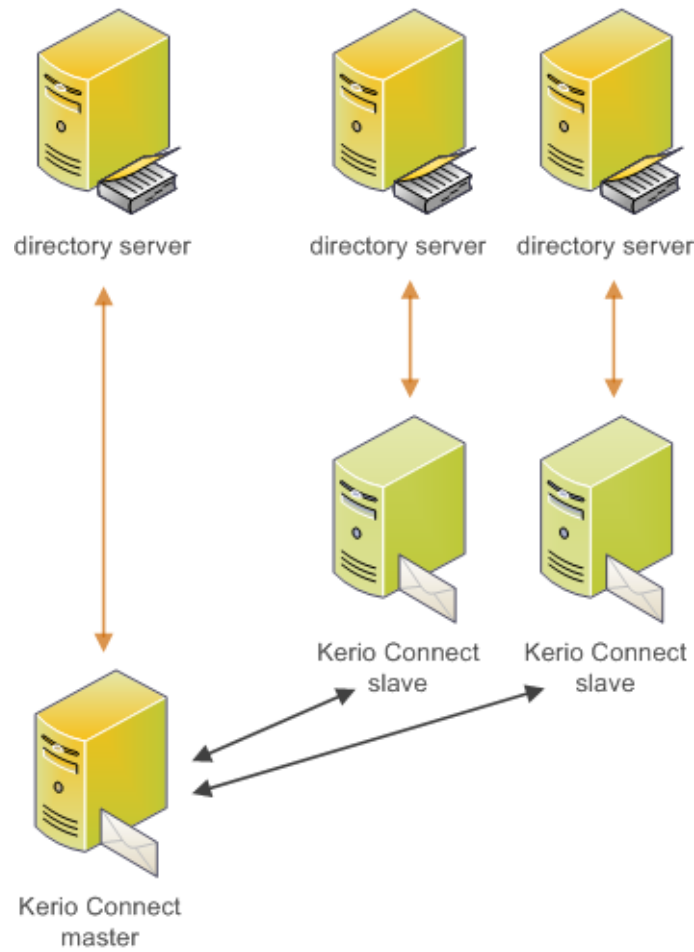
Figure 4.1   User management scheme

Note:
It is recommended to use a separate directory server for each server.
If you use a single directory server for multiple servers in the distributed domain, make sure that the traffic is fast enough between the servers and the directory service.

4.3 Forwarding mail and data sharing

Forwarding emails to the server with the users mailbox, requests for the Free/Busy server and resource administration are not managed by any of the servers. Each server sends the update to other servers. The communication is therefore peer-to-peer (see figure 4.2).
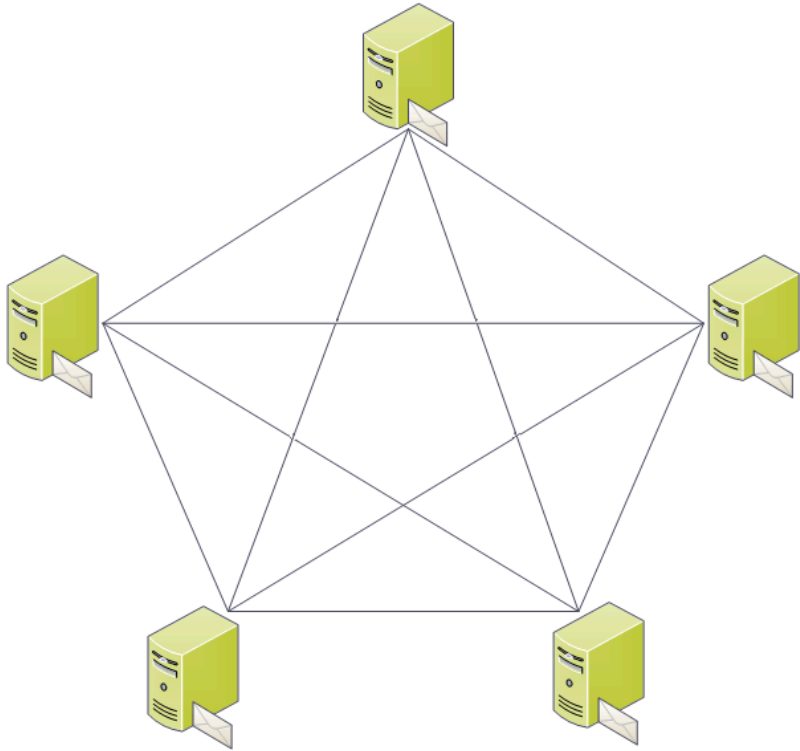
9

Figure 4.2 Forwarding emails, Free/Busy information and resource planning scheme

Chapter 5
Distributed domain setting

You do not have to set any of the servers as master or slave. It will be done automatically by connecting the slave servers to their master. Decide which of the servers will be master (see section 4.2).

Generally, two scenarios may occur that will be described in the following chapters:

- You have just purchased *Kerio Connect* and want to install it at several offices which should be interconnected via the distributed domain.

- You have been using several *Kerio Connect* servers and now you want to interconnect them via the distributed domain.

5.1 Clean installation of the servers and their interconnection via the distributed domain

The scenario is as follows:

- Your company has just installed clean copies of Kerio Connect at the headquarters (*mail.company.com*) and two branch offices (*newyork.company.com* and *seattle.company.com*).

- You want to interconnect all the servers via an only distributed domain called *company.com*. Select the server at the headquarters as the master.

The easiest way to do that is to create a local domain *company.com* on the very master server and map users and groups to the domain from the directory service. Then add the distributed domain on the other servers — connection to the master server and the new domain at the branch office will be created within a single operation.

On the master server (at the headquarters with server *mail.company.com*), set the following parameters:

1. Under *Configuration → Domains*, add a new local domain called *company.com*.

2. Now map users from the directory service to this domain.

Other settings must be done on the other servers (slave servers):

1. In *Configuration → Domains*, click on *Add → Distributed Domain*. The first page of the wizard gets opened providing information on how to proceed: Click on *Next*.

2. Enter DNS name of the master server and username and password of a user with admin rights for the master server (see figure 5.1). Click on *Next*.
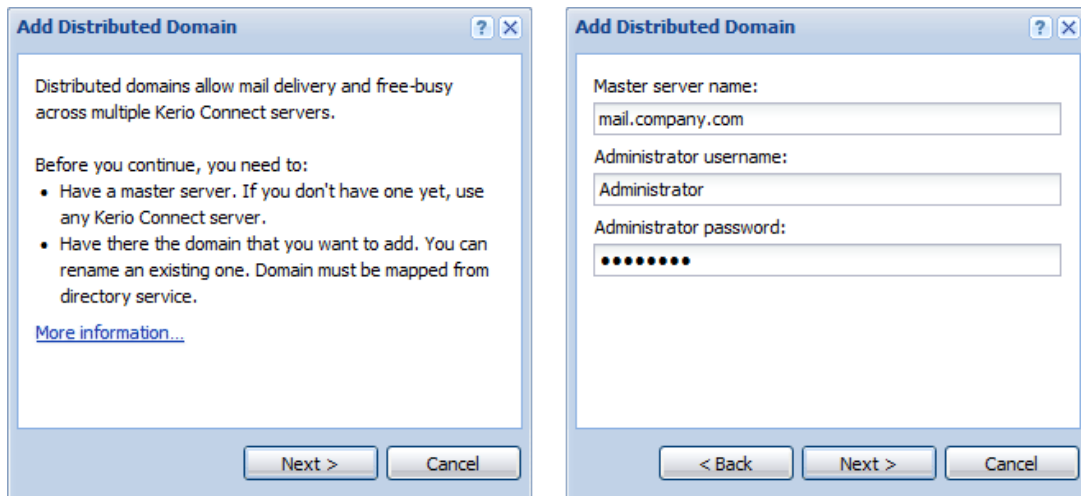
Figure 5.1 Adding a distributed domain

3. Now select a domain to be added (*company.com*) and click on *Finish* to complete the process.

    Copies of the *company.com* domain will be created on slave servers from the original on the master server (including configuration).

4. In the domain list under *Configuration → Domains*, a new column (*Distributed*) appears providing the information whether the domain is distributed or not.

    If the distributed domain has been added correctly, the icon next to the distributed domain name in section *Configuration → Domains* is red (see figure 5.2).

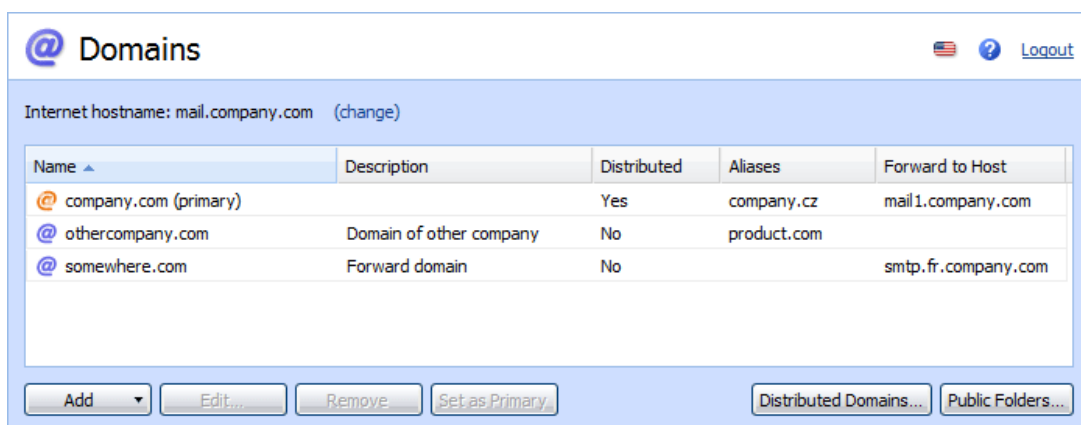
Figure 5.2 List of domains with a distributed domain

Note:
Another method is to create a local domain (with an identical name and directory service) on all servers and then connect them to the master server.

5.2 Interconnecting existing servers via distributed domain

The following scenario will be used as example:

- The company uses server *mail.company.com* with domain *company.com* at the headquarter and two branch offices with servers *newyork.company.com* (domain *newyork.company.com*) and *seattle.company.com* (domain *seattle.company.com*).

- All the servers are connected to the same LDAP server.

- You want to interconnect all the servers via an only distributed domain called *company.com*. Select the server at the headquarters as the master.

Since there are email domains that are supposed to be kept (so that it is not necessary to create new ones), it is necessary to rename these domains.

It is recommended to rename domains at the branch offices (i.e. *newyork.company.com* and *seattle.company.com* to *company.com*) and then connect servers at the offices to the master server at the headquarters (*mail.company.com*).

In the administration interface of servers *newyork.companyncom* and *seattle.company.com*, set the following parameters:

1. Rename domain *newyork.company.com* (and *seattle.company.com*) to *company.com*.

2. After server restart, go to *Configuration → Domains*.

3. Click on *Distributed domains* the wizard's first page providing information on how to proceed: Click on *Next*.

4. Enter DNS name of the master server and username and password of a user with admin rights for the master server (see figure 5.3) and click on *Connect*.
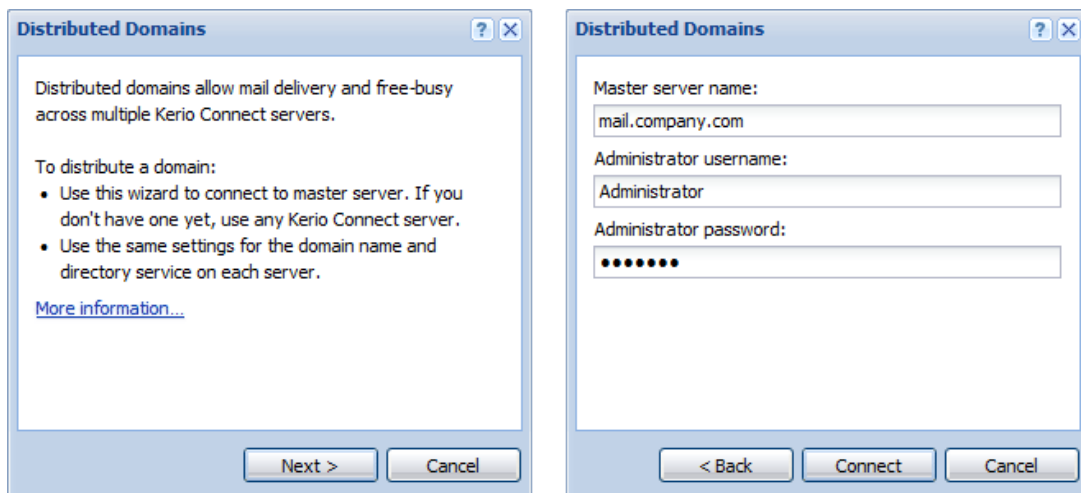

Figure 5.3 Connection to distributed domain

5. The server will connect to the distributed domain.

   In the domain list under *Configuration → Domains*, a new column (*Distributed*) appears providing the information whether the domain is distributed or not.

   If the confuguration is correct, the icon next to the distributed domain name in *Configuration → Domains* will get red on all the servers (see figure 5.2).

Chapter 6
Renaming distributed domains

If you wish to rename the distributed domain, follow these instructions:

1. Disconnect all servers from the distributed domain (see chapter 7).

2. On each server, rename the domain to your desired name.

3. Connect all servers to the distributed domain again (see chapter 5.2).

> *Warning:*
> Do not forget to first restart the server after you rename the domains and then reconnect them to the distributed domain.

Disconnecting server from distributed domain

To disconnect a server from the distributed domain, use the *Distributed domains* button in section *Configuration → Domains*. Only slave servers can be removed. Once the last slave server is disconnected, the distributed domain is removed automatically.

In *Configuration → Domains*, click on the button to open the *Distributed Domains* dialog and click on the *Disconnect this server from master* (see figure 7.1).
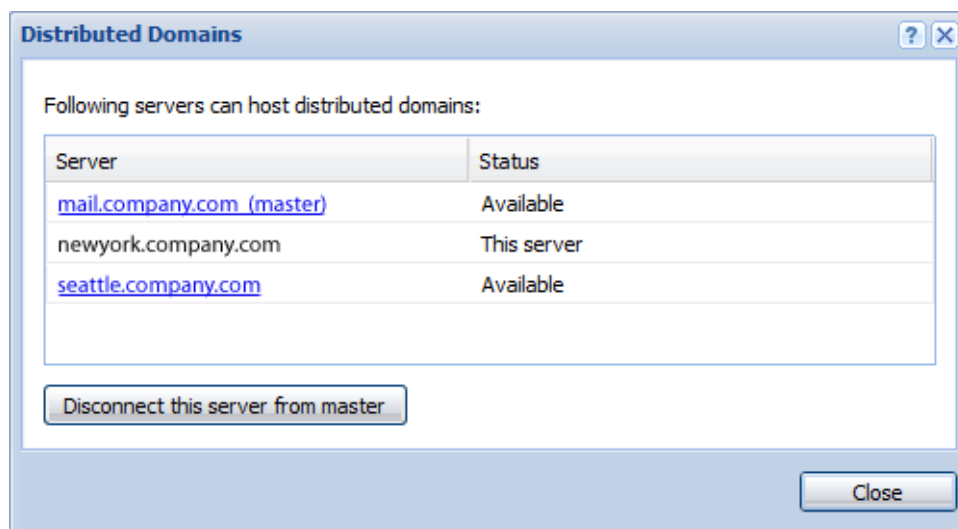

Figure 7.1 Disconnection from the master server

> *Warning:*
> The domain can be disconnected only through its own administration interface. If you are connected to a different server, click on its name in *Configuration → Domains → Distributed Domains*. A Kerio Connect Administration login page for this domain will open in your browser.

Chapter 8
User accounts in distributed domains

If you use the distributed domain, you administer all users in a directory service. To add a new account to the distributed domain, it is necessary to map it from a directory service. To remove a user from the distributed domain, follow the standard procedure.

You can still add local users to any of the servers. However, they will not belong to the distributed domain and no chages in these accounts will be revealed in the directory service. Local users will be able to use resource planning,Free/Busy server and such but only with accounts of the same server. Users from other servers will not "see" them.

For administration of domain aliases, mailing lists and resources, please use always the administration interface on the home server.

Warning:

Even though you can keep creating and administrating local items in distributed domain, it is strongly recommended not to do that. However, it can be beneficial to have one local administration account to which it will be possible to connect in case that for example a directory service server is not available.

Chapter 9
Administration of distributed domains

Administration roles in distributed domain are as follows:

Kerio Connect administrator

User with rights set as *Whole server read/write*.

- This user can connect servers to and disconnect them from the distributed domain.

- The user can also view, edit and migrate users mapped from the directory service on all the servers in the distributed domain.

Administrator of their domain

Users with rights set as *<your.domain> accounts*:

- The user can also view, edit and migrate users mapped from the directory service on all the servers in the distributed domain.

Chapter 10

Migration of user mailboxes in distributed domains

Kerio Connect allows you to move a mailbox physically from one server in distributed domain to another one (this option is useful when an employee is moving to a different company branch).

> *Warning:*
> Before migration, it is not necessary to shut servers down. However, it is recommended to make a full back-up of the data store.

10.1 Recommendations

- We advise to perform the migration at night or at the weekend, because it may be very time-consuming (depending on the number of user accounts and message store size).

- The user login will not be possible during the account migration. Messages which are delivered during the migration will remain in the queue and will be delivered to the new server after the migration.

10.2 Settings

Perform migration on the server to which you want to move the user accounts. Log in the Kerio Connect Administration interface as an administrator.

1. Under *Accounts → Users*, select one or more users to migrate (migratable accounts have the *Migrate Here* button active).

2. Clicking on *Migrate Here* starts migrating mailboxes to the target server. Mailboxes will be moved one by one.

The *Home server* column shows migration status of the accounts (see figure 10.1):

Migration can be cancelled by the *Cancel migration* button, if necessary. All temporary files will be removed and the mailbox will stay unchanged on the original server.

After the migration of each account, the administrator gets a message with information about:

- migration result (Completed successfully, Error, Canceled),

- time of the migration,
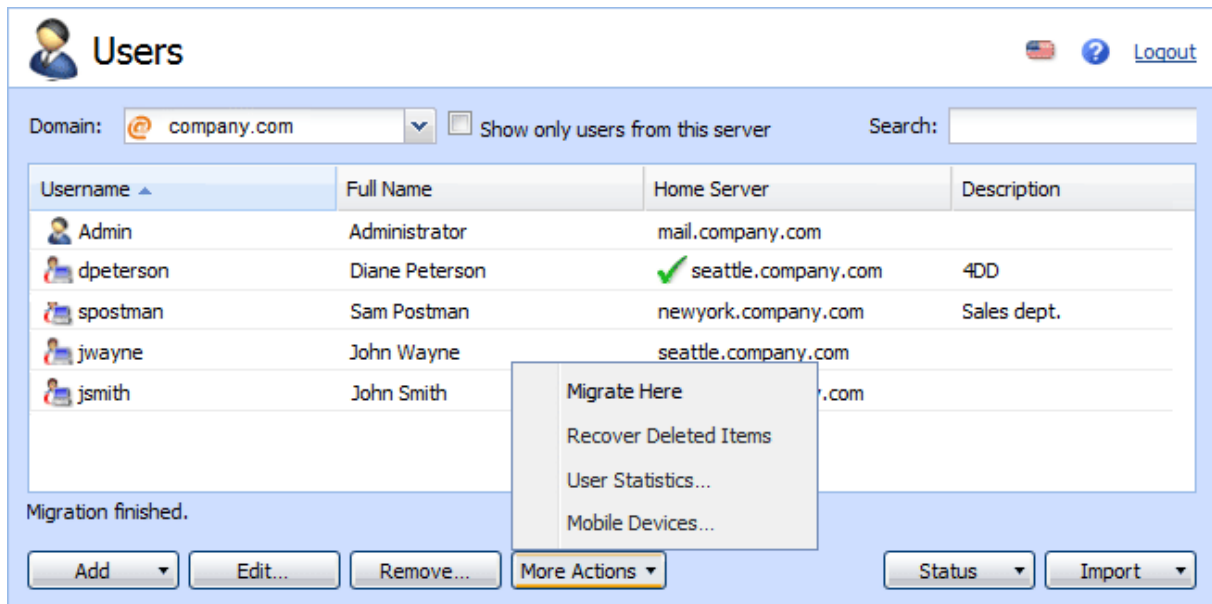
- size of the migrated mailbox.

Figure 10.1 User migration

If the migration is successful, perform a new full backup (especially when diferential backup is set).

To see which users (either local of from a directory service) have their account physically on the current server, check *Show only users from this server* on the right side of the distributed domain in the upper section of *Accounts → Users*.

> *Warning:*
> If the migrated user shares any folders with local users (users that are not members of the distributed domain), they will not be able to "see" from the new server.

Chapter 11
Communication problems

If connection to the master server is down, then:

- all slave servers can communicate with each other locally,

- incoming and outgoing email will be queued until connection to the master server gets restored.

If connection with any slave server is down, then:

- users from this server will be unavailable unless the server connection gets restored,

- incoming email for these users will be queued,

- activity of the other slave servers and the master server will not be affected.