

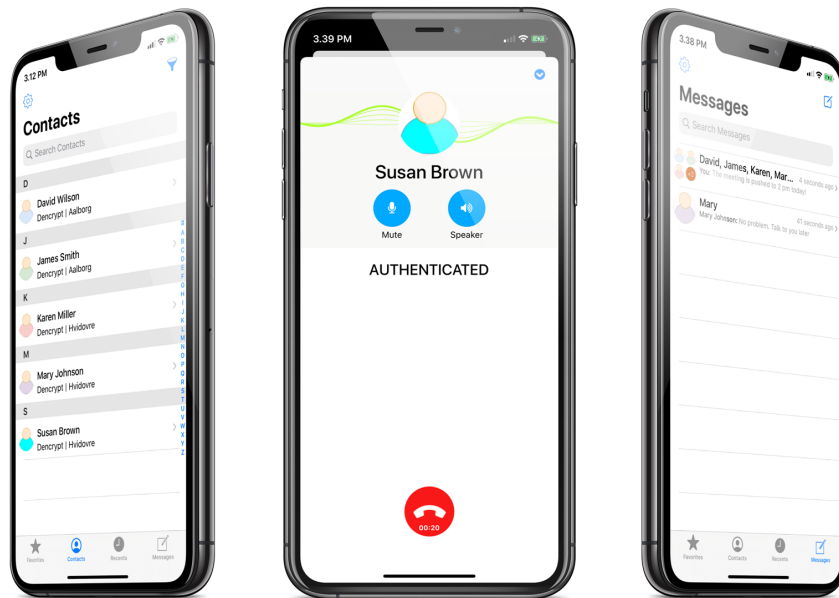


Dencrypt Communication Solution

Operational User Guide

Dencrypt Server System
5.4.0

v.1.3



6 February 2023

Public

Contents

Product versions	4
1 Introduction	4
1.1 Content	4
1.2 System architecture	5
1.3 Operational modes	6
1.4 Authenticated connections	6
2 Security instructions	7
2.1 Administrators	7
2.2 Secure IT environment	7
2.3 Federated systems	7
2.4 End-users	7
2.5 Provisioning	8
2.6 Lost or stolen devices	9
2.7 How to deactivate an account's access	9
2.8 Server Identity Verification	9
2.9 System Access	10
2.10 First time access for administrator	10
2.11 Password Policy	11
2.12 Install the browser certificate	12
2.13 Roles and Permissions	12
2.14 Audit logs	14
3 Phonebook	15
3.1 Basic concept	15
3.2 Allocate users to contact groups	15
3.3 Linking contact groups	16
3.4 Example 1: Contact groups reflecting functions	19

3.5	Example 2: Contact groups representing hierarchy	21
3.6	Recommendations	21
4	Teams	23
5	Emergency contacts	23
6	Dencrypt Server Bridge	24
6.1	Establish a server federation	24
6.2	Share users across systems	24
6.3	Shared data	25
6.4	Revoke a remote system connection.	25
7	Functionality in operational mode	27
7.1	Error message handling	27
7.2	Login	28
7.3	Home screen	29
7.4	Verify version number	29
7.5	Change Password	30
7.6	Users	30
7.7	Manage contact groups	40
7.8	Teams	42
7.9	Emergency contacts	44
7.10	Departments	46
7.11	Companies	47
7.12	Import users	49
7.13	Administrators	50
7.14	Calls statistics	54
7.15	Message statistics	55
7.16	Download browser certificate	58
7.17	License management	59
7.18	Apps	61

7.19	Standard Messages	62
7.20	Custom Attributes	63
7.21	Audit logs	65
7.22	Password policy	66
7.23	Server status	67
7.24	Manage bridge connections	68
7.25	Certificates	69
7.26	Features	72
7.27	Manage alerts	73
7.28	Manage backup	74
7.29	Display operational mode	75
8	DSS REST API	77
8.1	API endpoints	77
8.2	Authentication	77
8.3	Examples	77
A	Advanced management functions	80
A.1	Change of operational mode	80
A.2	Dencrypt Control Center: Configuration	81
A.3	Dencrypt Certificate Manager: Configuration	81
A.4	Dencrypt Provisioning Server: Configuration	83
A.5	Dencrypt Database: Configuration	84
A.6	Dencrypt Communication Server: Configuration	85
A.7	Dencrypt System Bridge: Configuration	86
A.8	Features configuration	88
A.9	SSH access	89
B	Audit logs definitions	90
C	Version history	93

Product versions

This guide applies to Dencrypt Server System 5.4.0 , which consists of the following components:

- Dencrypt Certificate Manager (DCM),
- Dencrypt Provisioning Server (DPS),
- Dencrypt Control Center (DCC),
- Dencrypt Database (DDB),
- Dencrypt Communication Server (DCS),
- Dencrypt System Bridge (DSB).

1 Introduction

1.1 Content

This guide is intended for administrators of the Dencrypt Server System and provides instructions on how to operate the server system and securely manage end-users. All administrators of the server system shall familiarize themselves with this document before using the product. The contents of this document are as follows:

- Overview of the system and its components.
- How to access the server system.
- Administrator roles and associated permissions.
- How phonebooks are generated.
- Security considerations.
- Detailed description of all server functionality.
- Error messages and how to respond to them.
- How to manage log events.

1.2 System architecture

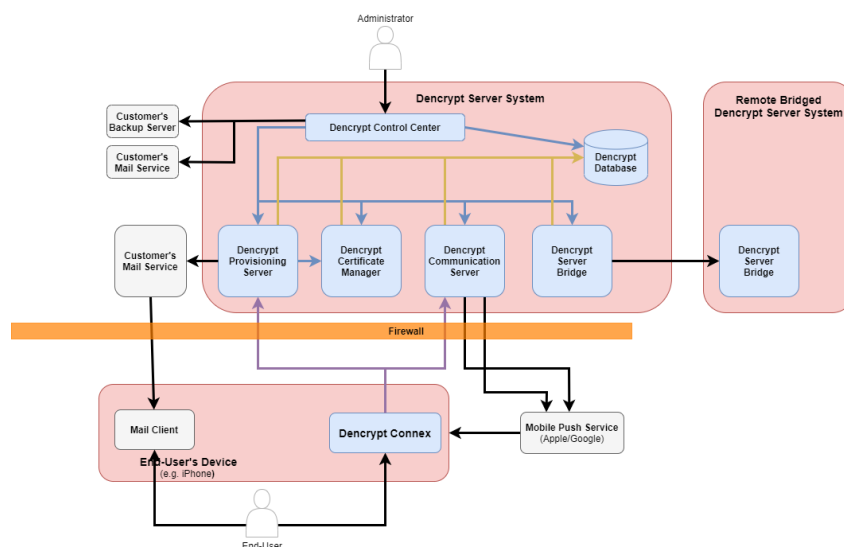


Figure 1: Overview of the Dencrypt Communication Solution

The Dencrypt Communication Solution is shown in Figure 1 and consists of a client application installed on the end-user's mobile device and the Dencrypt Server System deployed within a secure IT environment. The Dencrypt Communication Solution consists of the following components:

- **Dencrypt Connex**

Dencrypt Connex is the mobile client that provides secure voice and instant messaging using the SIP protocol. The client must be provisioned before it can be used. This is done via the Dencrypt Provisioning Server.

- **Dencrypt Provisioning Server (DPS)**

The Dencrypt Provisioning Server (DPS) is used to initialize clients with credentials and client certificates to communicate with the system's server. An HTTPS web link is provided to the client for initialization. The link is securely delivered to the end-user and is disclosed during transmission. The DPS provides the means for secure transmission.

- **Dencrypt Communication Server (DCS)**

The Dencrypt Communication Server (DCS) provides the SIP services required by clients to establish secure voice calls between two or more clients and exchange messages between clients. The system supports multiple instances of the DCS to provide logical redundancy and load balancing. The DCS is also responsible for generating and distributing phonebooks and settings to the clients. The DCS includes a LiME server to facilitate a key exchange for secure messaging.

- **Dencrypt Database (DDB)**

The Dencrypt Database (DDB) provides database services to the system. It stores data and logs for end-users, statistics, servers and connections. It also stores secure messages awaiting delivery and facilitates the key exchange protocol.

- **Dencrypt Control Center (DCC)**

The Dencrypt Control Center (DCC) is used for user management and server administration. This includes creating/deleting users and managing contact groups. The DCC provides a web interface that can be accessed via a web browser from the administrator's local machine.

- **Dencrypt Certificate Manager (DCM)**

The Dencrypt Certificate Manager (DCM) is the central point for TLS certificates in the system. After provisioning, all connections between Dencrypt Connex and the Dencrypt Server System use mutually authenticated TLS connections. The required TLS certificates are issued by the Dencrypt Certificate Manager. The DCM also issues TLS certificates for internal server validation.

- **Dencrypt System Bridge (DSB)**

The Dencrypt System Bridge (DSB) handles all communication between external Dencrypt systems. It is used as a gateway to federated systems, including certificates for mutual authentication towards external Dencrypt Server Systems.

1.3 Operational modes

The Dencrypt Server System can be operated in two modes:

- **Operational mode** Used for daily system and user management. This mode is operated by the customer organization using the User Admin, Company Admin, and System Admin roles [Roles and Permissions 2.13]. The functionality available in Operational Mode is described in detail in [Functionality in operational mode 7].
- **Maintenance mode** Used for service and maintenance updates. This mode is operated by trained Dencrypt personnel (or Dencrypt partners) via the Service Access role [Roles and Permissions 2.13].

1.4 Authenticated connections

All connections between Dencrypt Connex and the Dencrypt Server System (DSS) are mutually authenticated TLS connections. The Dencrypt Certificate Manager (DCM) issues intermediate certificates that are signed by the Dencrypt Root CA and distributed by the Dencrypt Provisioning Server (DPS) or the Dencrypt Communication Server (DCS).

1.4.1 Server validation

Server certificates issued for external TLS connections are also used for internal connections between server components. The Dencrypt Control Center is authenticated by the administrator's browser [Server Identity Verification 2.8].

1.4.2 App validation

A signed certificate on the Dencrypt Connex client is created by the client sending a certificate signing request to the Dencrypt Provisioning Server (DPS), which returns the client certificate in the response.

2 Security instructions

2.1 Administrators

The personnel operating the Dencrypt Server System must be trained and trustworthy IT professionals. Specifically, an administrator should:

- Be trusted by the organization, be non-hostile, be able to follow its instructions, and have been trained to perform their actions in accordance with its instructions and security policies.
- Be authorized by the organization to operate the system with the managerial role assigned to them [Roles and Permissions 2.13].
- Have received training in the secure operation of the Dencrypt Server System.
- Be familiar with this document and the procedures for the secure operation of the system.

2.2 Secure IT environment

The Dencrypt Server System must be operated in a physically secured IT environment with a local network dedicated to the use and functionality of the system. The IT environment must provide a well-configured firewall to protect the Dencrypt Server System from untrusted networks. The device used to operate the Dencrypt Control Center must be well-configured and located in a secure environment. It must be accessible only to trained and authorized personnel and must not be exposed to other users or potential attackers.

2.3 Federated systems

Federation of Dencrypt Server Systems is possible using the Dencrypt Server Bridge, which allows for secure communication between end-users from different organizations [Dencrypt Server Bridge 6].

Before establishing a bridge connection to a remote system, ensure that:

- The remote Dencrypt Server System shall be trusted and operated in a secure manner.
- The System Administrator of the remote system meets the requirements listed in [Administrators 2.1].
- The exchange of *Connection Requests* is secured using encrypted email or hard drives and is not disclosed to third parties [Establish a server federation 6.1].

If there is evidence or reasonable suspicion that any of these criteria are no longer met, the connection to the remote system is immediately revoked [Revoke a remote system connection 6.4].

2.4 End-users

End-users are the users of the Dencrypt Connex client. End-users must be trusted, non-hostile and trained to perform their actions in accordance with their instructions and security policies.

2.5 Provisioning

End-users must complete an initial registration (provisioning) process before they can begin using the application.

From the user profile on the administration page, an email invitation can be sent to the mobile client [Send invitation 7.6.9]. The invitation provides the end user with a one-time activation link (URL or QR code) for system registration. The delivery process of the activation link must ensure the confidentiality of the link. In case of eavesdropping, an adversary could be impersonated as the user for whom the activation link was intended. The invitation email must be delivered in a secure manner: either using encrypted emails or within a locally secured network.

The end-user account must be immediately deactivated if there is any suspicion that the invitation email may have been disclosed to an unauthorized person or otherwise compromised.

See [How to deactivate an account's access 2.7] for details on how to deactivate a user.

The web link can only be used once and will expire after a limited period of time. When this happens, the end user receives an "Invite error" message and is prompted to contact the system administrator. In this case, the administrator must perform the following actions to verify that the end user is not already registered on the server:

Verification of correct provisioning

-
- Step 1: Login to the Dencrypt Control Center and select *Administration -> Users*.
 - Step 2: Identify the end-user and verify the status of the relevant app. If the status columns are not shown, press the edit icon and select 'Status'.
 - Step 3: If the registration status is *Registered* and the end-user application is not activated, a potential attacker may have used the invitation to register on the system. Deactivate the account immediately.
 - Step 4: If the registration status is *Invited*, an error may have happened during the provisioning process. The user can safely be provided with a new invitation email.
-

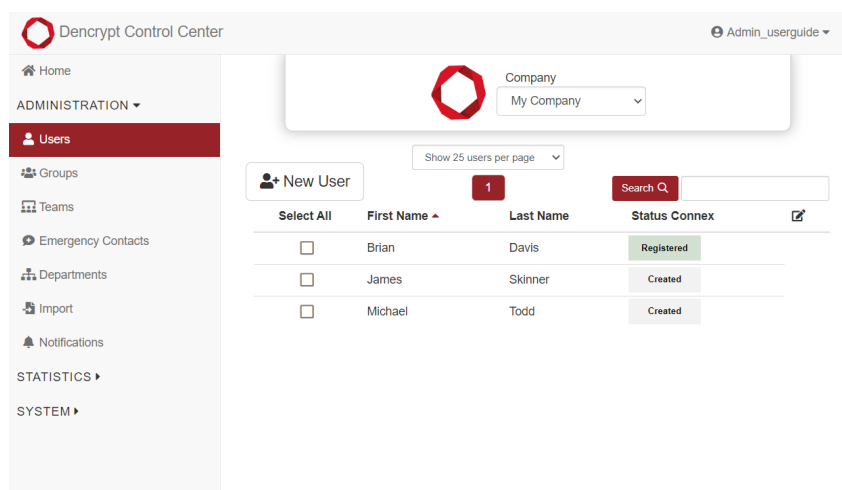


Figure 2: Verification of registration status

End-user provisioning is required for the initial creation of a user account but is typically not required for system updates.

2.6 Lost or stolen devices

Each end-user must immediately report to the system administrator if a device is lost, stolen, or otherwise compromised.

The system administrator must immediately deactivate the user account to prevent unauthorized access.

See [How to deactivate an account's access 2.7] for details on how to deactivate a user.

2.7 How to deactivate an account's access

If a user's device or account is suspected of being compromised, it should be deactivated to prevent unauthorized access. To deactivate a user account (Figure 3):

Deactivate user account

- Step 1: Open *Administration* -> *Users* in the left menu.
- Step 2: Select the company the user is part of, in the dropdown.
- Step 3: Select the user to open the detailed user information.
- Step 4: Open the *Remove* tab.
- Step 5: Select *Deactivate* and confirm the warning.

The user account will no longer be able to access the system. New invitations can be sent to the user to restore access.

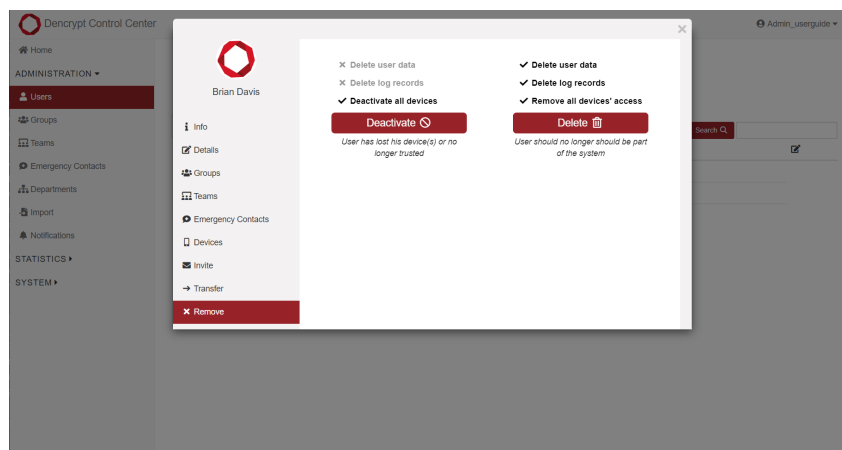


Figure 3: Deactivate a user's access

2.8 Server Identity Verification

To verify the server's identity, the root certificate must be installed as a trusted certificate in the administrator's browser. See [Install the browser certificate 2.12] for instructions on installing the certificate.

2.9 System Access

The administration of users and server components is managed from the Dencrypt Control Center (DCC). It provides an easy way for adding, editing, and changing end-user data and phonebook contacts and for the system configuration.

The DCC is accessible using a web browser (Chrome is recommended). The computer used to access the DCC shall be well-configured, located within a secure local network and may not be exposed to unauthorized users or persons.

For service and maintenance, the server components are also accessible using an SSH connection from within the Customer's secure IT environment. The SSH access shall only be used for maintenance by Dencrypt technical personnel or IT professionals, who have received training in installing and configuring a Dencrypt Server System (see [SSH access A.9]). The SSH connection is implemented using the SSH-2 protocol that relies on OpenSSL for the cryptographic primitives.

2.10 First time access for administrator

The first access to the Dencrypt Control Center will happen from a browser without a Dencrypt certificate and with a temporary, one-time password. Follow the steps below to access the system, change their password and install the root certificate in the browser:

First time access for administrators

- Step 1: A URL to the Dencrypt Control Center and login credentials have been received.
 - Step 2: Enter the URL for the DCC in the web browser's address bar.
 - Step 3: A privacy warning will be displayed in the browser with the text "Your connection is not private". Please acknowledge the warning by tapping "Advanced" followed by "Proceed to (URL)" (See example in Figure 4).
 - Step 4: Enter login credentials.
 - Step 5: At the first login, the administrator is asked to change his/hers password.
 - Step 6: Download and install the Dencrypt certificate to verify server identity (Follow the instructions in [Install the browser certificate 2.12])
-

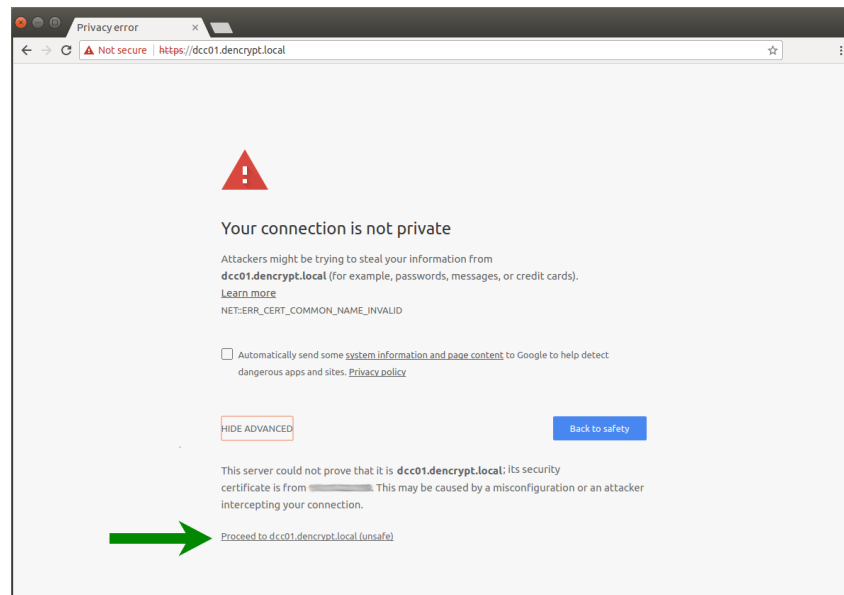


Figure 4: Browser warning for first time access without certificate installed

All login and management events are logged for review by the System Admin [Audit logs 2.14].

2.11 Password Policy

At the first login, the administrator will be prompted to change their password. If this is not the case, the credentials may have been compromised. Contact the System Administrator immediately to have your account locked to scan logs for any unauthorized login attempts.

The password created upon the first login is personal and must never be shared with anyone. Support will never ask for your password. It is recommended not to store the password, but if necessary it must be stored securely. Do not save it in plaintext but use recognized encryption tools for password storage.

If a password is forgotten, it can be reset by a system administrator (see [Lock and password reset 7.13.5]).

The password policy can be configured to comply with local policies [Password policy 7.22]. The following minimum requirements are recommended:

- A minimum length of nine characters.
- Use of both upper-case and lower-case letters.
- Include at least one digit.
- Include at least one special character.
- Do not use passwords that are easy to guess such as 'password' or '1234'.
- Do not use passwords that are associated with your identity: birthdays, names or addresses.

If the password is lost or compromised, contact the System Administrator immediately to have your account locked. If an administrator repeatedly fails to authenticate, the account will automatically be locked. Contact the System Administrator to have your account unlocked.

A System Administrator can unlock the account as described in [Lock and password reset 7.13.5].

2.12 Install the browser certificate

To validate the server identity, follow the instructions below to download and install a browser certificate.

Install browser certificate.

Step 1: Open *System* -> *Browser Verification* and select *Download As File*.

Step 2: The certificate file *root-certificate.crt* is stored to the local computer.

Step 3: Install the certificate following the instructions of the OS and browser:

- Windows: <https://support.globalsign.com/ssl/ssl-certificates-installation/import-and-export-certificate-microsoft-windows>
- MacOS: <https://www.ssllsupportdesk.com/how-to-import-a-certificate-into-mac-os/>

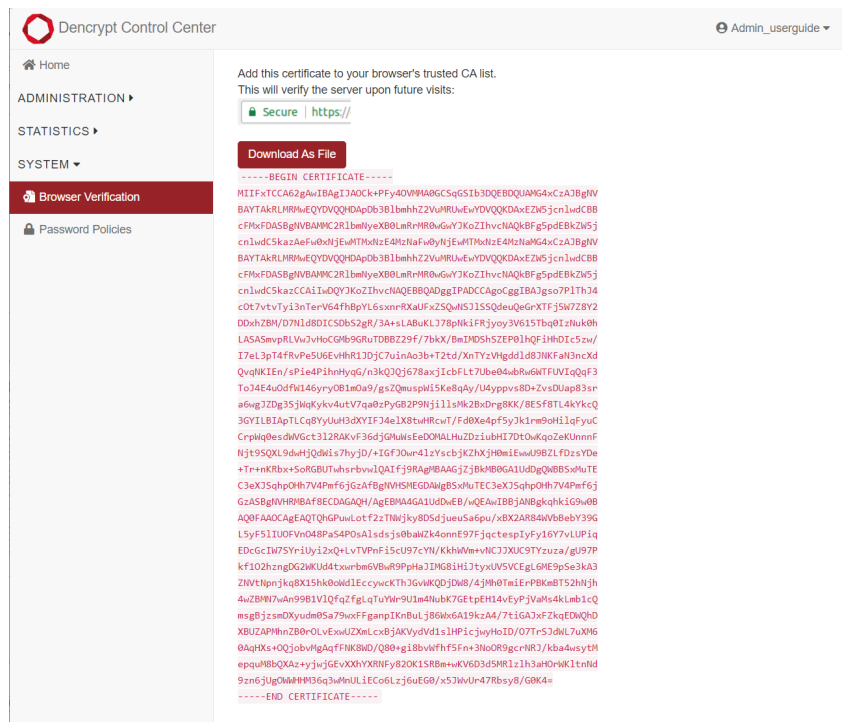


Figure 5: Download Browser Certificate

2.13 Roles and Permissions

The system allows for different roles in the administration of the DCC. The roles are hierarchical meaning each role has incremental privileges.

Role	User admin	Company admin	System admin	Service access
Features	Operational Mode			Maintenance Mode
User management	Access ¹	Access	Access	Access
Statistics	Access ¹	Access	Access	Access
Company management	No access	Access	Access	Access
License management	No Access	Access	Access	Access
Administrator mgmt	No Access	Access ²	Access ³	Access
Audit logs	No Access	No Access	Access	Access
System configuration	No Access	No Access	Read Only	Access

¹ For allocated companies only.

² Can create user admin accounts only.

³ Can create user admin, company admin and system admin accounts.

Table 1: Roles and Permission.

2.13.1 Role: User admin

The *User admin* role is used in operational mode to manage end-users within a company. The *User admin* can perform actions on end-users within the allocated companies:

- User management: Create, edit and remove users.
- Provisioning of users.
- Contact group management
- Setup emergency contacts

The role is explicitly granted to each assigned company by a higher-level administrator. The role is provided for user management within specific companies only.

2.13.2 Role: Company admin

The *Company admin* role is used in operational mode for managing companies and end-users across companies. In addition to the permission of the *User admin*, the *Company admin* can:

- Company management: Create, edit and remove companies.
- Define standard messages.
- Upload license files
- Create, delete and modify administrators of User Admin role.

The role is provided to administrators to manage users and user administrators across all companies.

2.13.3 System admin

The *System admin* role is used in operational mode for daily system operation and monitoring. In addition to the privileges of the *User admin* and *Company admin*, the *System admin* has access to:

- Monitor the technical status of the server system.

- Analyze logs for system events.
- Create, delete and modify administrators of *User admin*, *Company admin* and *System admin* roles.

The role is provided to local system administrators.

2.13.4 Service access

The *Service access* role is used in maintenance mode for system maintenance and updates. The role is restricted to Dencrypt technical support and service partners and should not be used for daily operations. The *Service access* role may:

- Configure system parameters
- Certificate management
- Manage Dencrypt Server Bridge connections to other systems.
- Create, delete and modify administrators of Service Access roles.

The privileges of the *Service access* role are only applicable in maintenance mode.

2.13.5 Creating new administrators

To create a new administrator a unique username and one-time password must be provided. It shall be ensured that credentials are provided in a secure way to the intended person, such as by direct personal delivery or by using encrypted emails.

The new administrator will be prompted to change the password at the first login.

2.14 Audit logs

All system events are logged and can be audited [Audit logs 7.21]. It is important for system security to regularly monitor and analyze logs to prevent and detect misuse and possible security incidents. Log analysis is the responsibility of the System Administration and is recommended to include:

- Detection of repeated unauthorized login attempts.
 - Logged as 'LOGIN-ATTEMPT' in the DCC event log.
 - Logs of SSH and TLS connections are collected for each server and are available as downloadable files.
- Verification of authorized logins.
- Scanning for unusual or suspicious events related to user administration.
- Monitoring changes to the server configuration. Server configurations will only change during system maintenance.

3 Phonebook

The end-users' phonebook is individual and determined by contact groups defined within the Dencrypt Control Center. The concept of contact groups allows for the generation of complex structures defining which users can communicate. A user can only establish calls or exchange messages with contacts in their phonebook.

The phonebook is "closed" meaning that it is not possible to establish secure communications with individuals outside the phonebook nor is it possible for an end-user to add contacts to their phonebook. New phonebook entries need to be created by the system administrator.

This section describes how contact groups can be created to reflect the communication structures required and includes two examples to illustrate the concept. As the concept is very versatile, the section also includes recommendations for creating contact groups that fulfill the purposes and are manageable.

3.1 Basic concept

A contact group consists of one or more users within the same company. A contact group may be linked to other contact groups allowing the members of the two contact groups to communicate.

The simplest form is to create a single contact group containing all users as illustrated in Figure 6a. An inter-group link is by default created allowing the members to contact each other. To allow communication between users of different groups, a link is established connecting the two call groups as shown in Figure 6b.

The concept allows users to be members of multiple contact groups. There will only be a single instance of a contact in the phonebook even if multiple links exist.

Contact groups and their associated users are always established within a company but can be shared with other companies.

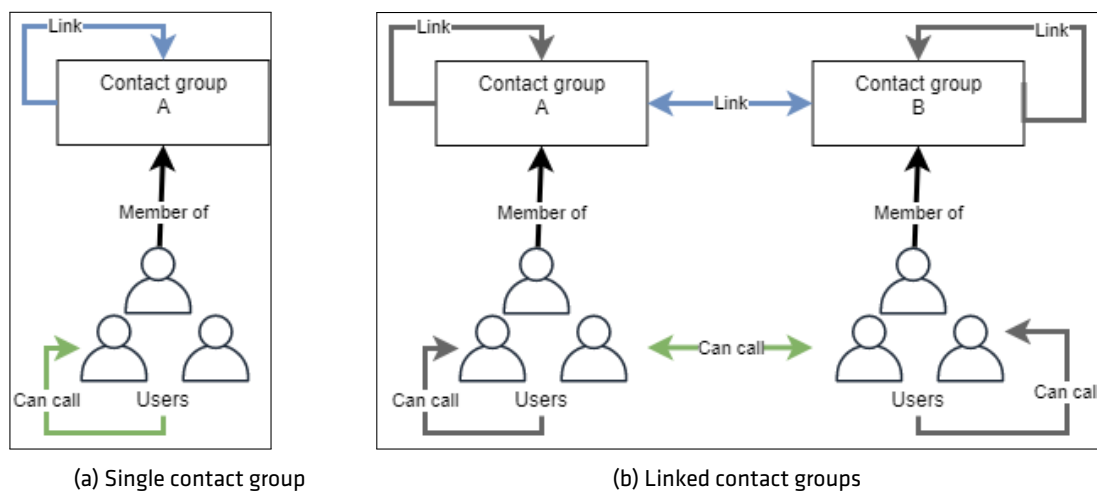


Figure 6: Contact group concept

3.2 Allocate users to contact groups

A user can be a member of any contact group within the company. A user can be allocated to contact groups during user creation or editing.

Allocate users to contact groups.

Step 1: Open *Administration* -> *Users*.

Step 2: Select the user.

Step 3: Select the *Groups*-tab.

Step 4: Check the groups of which the user shall be a member.

Step 5: Verify the phonebook content in the preview.

Step 6: Click *Save*.

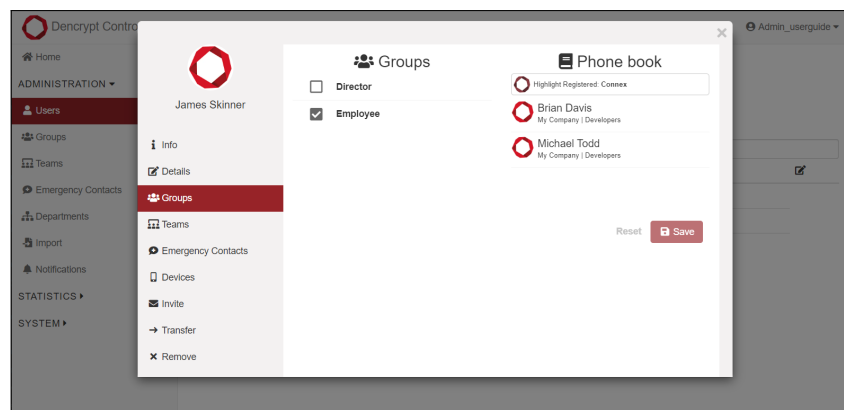


Figure 7: Allocate users to contacts groups.

The resulting phonebook is comprised of all the members of the linked groups. Contacts will appear only once; even if a contact is linked multiple times.

3.3 Linking contact groups

To create a link between two groups to allow their users to contact each other, do the following steps:

Linking contact groups

Step 1: Open *Administration* -> *Groups*.

Step 2: Select one of the contact groups to be linked.

Step 3: Find the other contact group in the list and select it.

Step 4: Select the relevant link attribute: None, In, Out or Both.

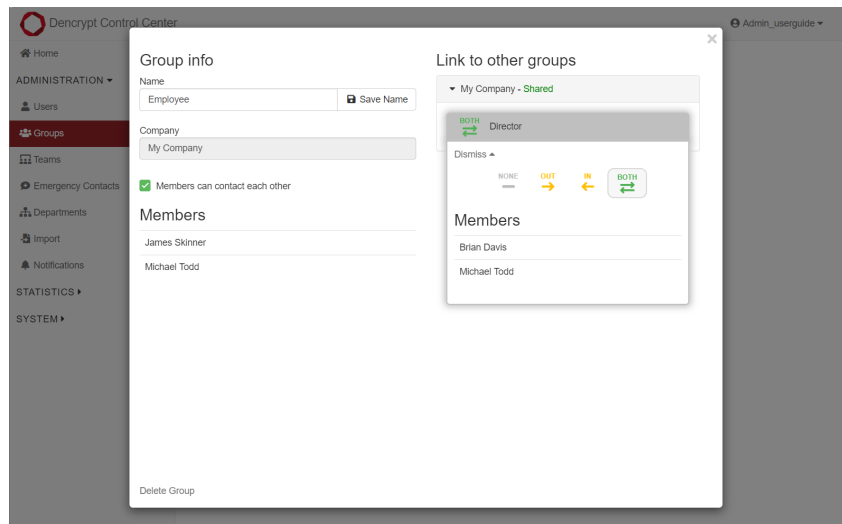


Figure 8: Linking contact groups.

The link attributes are:

- **NONE**: No contact is established between the groups.
- **OUT**: The members of the current group can contact members of the other group.
- **IN**: The members of the other group can contact the members of the current group.
- **BOTH**: Members of both groups can contact the opposite group.

3.3.1 Link to own contact group

By default, all the members of a contact group can contact each other. If this not desired, the link to the own group can be removed (Figure 8):

Remove link to own group.

Step 1: Open Administration -> Groups.

Step 2: Select the group to edit.

Step 3: Clear the checkbox: 'Members can contact each other'.

Step 4: Accept the warning.

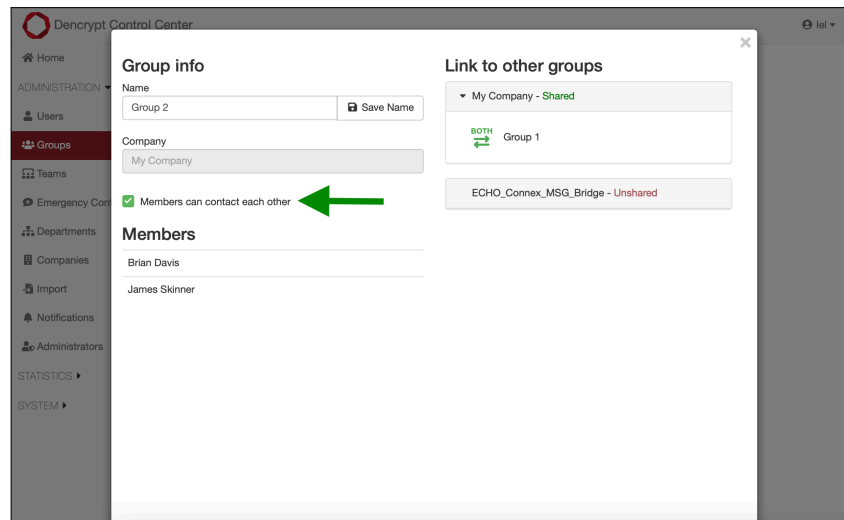


Figure 9: Remove link to own group.

3.3.2 Link groups across companies

By default, contact groups are only linked to contact groups within their own company. To allow contact groups to be linked with another company's contact groups, both contact groups must be shared with the opposite group's company.

The administrator must have access to modify both companies, which is either:

- A **User Admin** with explicit access to both companies.
- A **Company Admin**, a **System Admin** or a **Service Access**.

To share a contact group with another company, do the following steps:

Link contact groups between companies.

Step 1: Open Administration -> Groups.

Step 2: Select on the group to be shared.

Step 3: Locate the company in the list and click the **Unshared**.

Step 4: Accept the warning.

Step 5: The contact groups from the other company are now visible and can be linked [Linking contact groups 3.3].

Step 6: To unshare the company click the **Shared** and conform the warning.

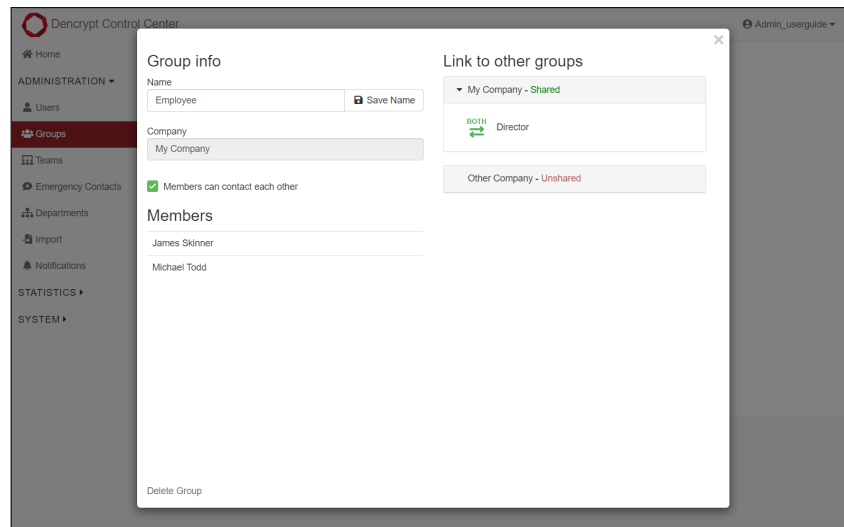


Figure 10: Link contact groups across companies

3.4 Example 1: Contact groups reflecting functions

Contact groups are structured according to the function of their members. In this example, **Company Alpha** consists of three functions:

- **Development** can contact **Management** and **Development** itself.
- **Sales** can contact **Management** and **Development**, but not **Sales** itself.
- **Management** can contact everyone.

Company Bravo has shared a contact group, **Executives** to allow communication at management level. The contact group structure is shown on Figure 11.

Example 1: Steps for creating contact groups

Step 1: Create the three call groups for Company Alpha and set attributes as:

- (a) **Development** - Apply BOTH link to Management and IN link to Sales Figure 12a.
- (b) **Sales** - Apply BOTH link to Managers and OUT link to Development and clear "Members can contact each other" Figure 12b.
- (c) **Management** - Apply BOTH link to Sales and BOTH link to Development Figure 13a.

Step 2: Set attributes for the shared contact group from Company Bravo:

- (a) **Executives** - Apply BOTH link to Management. Figure 13b and ensure that Development and Sales are "Unshared" or link type NONE is applied.

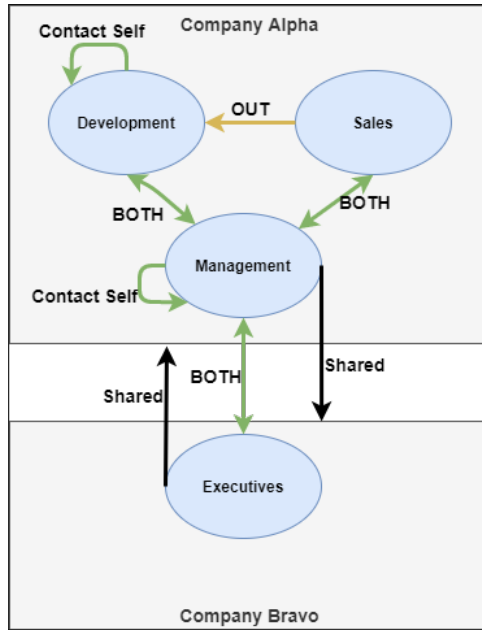
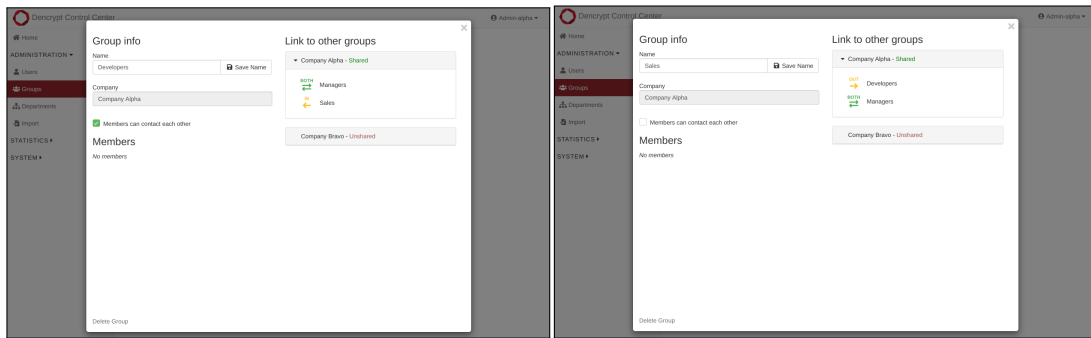


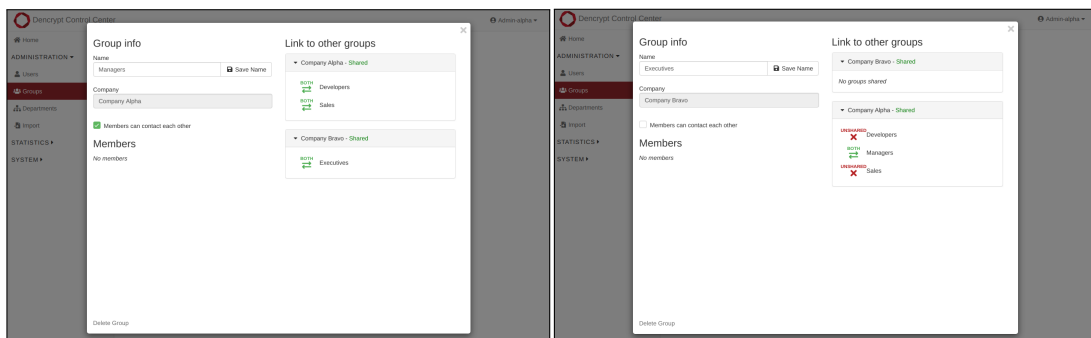
Figure 11: Example 1: Contact group structure based on function.



(a) Example 1: Development group settings.

(b) Example 1: Sales group settings

Figure 12



(a) Example 1: Management group settings.

(b) Example 1: Executives group settings

Figure 13

3.5 Example 2: Contact groups representing hierarchy

Contact groups may also reflect the hierarchy of an organization consisting of VIPs and ordinary members (Standard). The VIPs may call everyone in the organization, but can not be contacted by the ordinary members. In addition, a contact group is established for users shared with **Company Bravo**.

- **Standard** can only contact **Standard** itself.
- **VIP** can contact **Standard** and **VIP** itself.
- **Bravo Shared** can contact **Alpha Shared** from **Company Bravo**.

Figure 14 illustrates the communication structure. The steps for creating the contact groups are shown below.

Example 2: Steps for creating contact groups

Step 1: Create the three call groups for Company Alpha and set attributes as:

- Standard** - No additional links required.
- VIP** - Apply an OUT link to **Standard**.
- Bravo shared** - Share contact groups with **Company Bravo** and apply a BOTH link to **Alpha shared**. Clear "Members can contact each other".

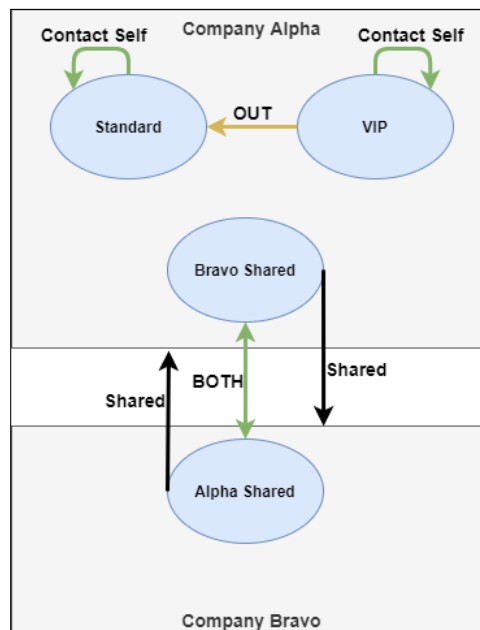


Figure 14: Example 2: Contact groups representing hierarchy.

3.6 Recommendations

The concept for contact groups offers a large flexibility in creating communication structure, but can also easily turn into very complex configurations with a lack of overview. To keep contact groups manageable, a few recommendations are provided:

- **Limit the number of contact groups:** A small number of contact groups are easier to maintain. If there is not a need for complex contact structures, use only a few call groups, with as many members as possible.
- **Limit the number of links:** Contact groups shall only be linked if there is a need. Consider, if groups can be merged.
- **Apply accurate naming:** Identify the commonality of the members within a contact group. It may be their function in the company, their hierarchy, project groups or even individual names. Naming groups accurately will ease the burden of associating new users with groups.

4 Teams

A *Team* is a chatroom managed by the system administrator. Teams may be created for a project team, a department or a mission, where there is a need for a common messaging channel and where members can join or leave.

When a user is allocated to a team, it will automatically appear in the app. Teams can be shared within companies when the administrator:

- Has *User admin* privileges for both companies.
- Has *Company admin* or *System admin* or *Service access* privileges.

5 Emergency contacts

Emergency contacts are defined to allow end-users to send emergency messages to a pre-defined contact. To set up a list of emergency contacts:

Define emergency contacts

Step 1: The administrator creates an emergency list [Create a new emergency list 7.9.1].

Step 2: Emergency contact(s) are added to the list [Allocate users to emergency list 7.9.2].

Step 3: The emergency list is allocated to the relevant companies.

6 Dencrypt Server Bridge

The Dencrypt Server Bridge component is used to federate Dencrypt Server Systems to allow communication between users on different systems.

The Federation requires that the system administrator establish mutual trust. Once two server systems are federated, each system administrators are in control of which companies and users are shared across systems. It may be the entire organization or a few individual contacts. The concept of contact groups also applies to the federated system for user sharing and creation of individual phonebooks [Phonebook 3].

The steps required to share across companies are listed below and detailed in the following sections:

Steps for sharing users across systems

Step 1: Federate systems by establishing mutual trust.

Step 2: Publish companies to be visible at the remote system.

Step 3: Share and link contact groups to make users visible at the remote system.

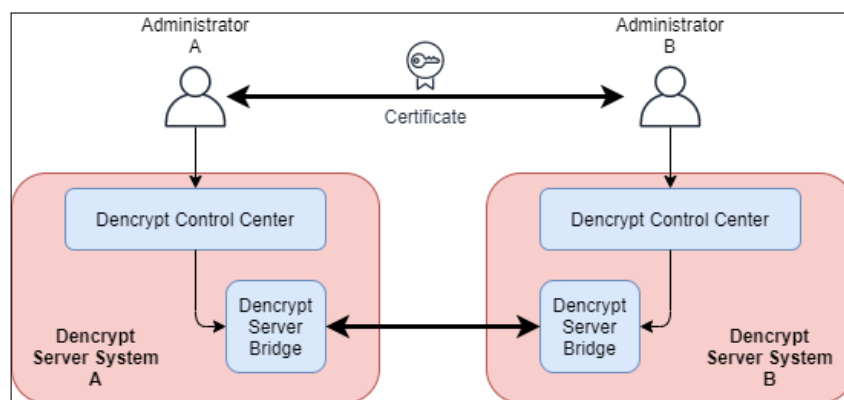


Figure 15: Dencrypt Server Bridge overview.

6.1 Establish a server federation

This operation requires the administrator to have *Service access* privileges. To federate two server systems, each system administrator will create a remote system and establish a trusted connection.

The process involves the system administrators exchanging and installing configuration files. Verify that the configuration file is not changed in transport.

See [Create a remote system connection A.7.1] for detailed instructions.

6.2 Share users across systems

Once two systems are federated, an administrator with at least *Company Admin* privileges can publish one or more local companies to be visible in the remote system. A published company becomes visible with the company name and logo only.

To publish a company, perform the following steps:

Publish a company

Step 1: Open *Administration* -> *Companies*.

Step 2: Select the company to be published.

Step 3: Select the remote system.

Step 4: Click *Save*.

When the remote system administrator has published one or more companies, it becomes visible on the *Administration* -> *Groups* page. The system administrator can now share and link contact groups in the same way as for local groups [Linking contact groups 3.3].

Notice: Both administrators have access to change the link type.

6.3 Shared data

The user data shared between federated systems are kept to a minimum and limited to phonebook metadata: Name, Company, Department and the unique user-id.

Remote companies and users are accessible to the administrator, but restrictions apply:

- Only the users of a remote-linked contact group are shared.
- Remote user details, departments and companies can not be edited or deleted.
- Remote users can not be provisioned or revoked.
- Remote users can not be invited, revoked or deleted.
- Remote user statuses are limited to "Created" and "Registered".
- Email addresses and phone numbers are not shared.
- User statistics such as calls, messages, last connected/invited/revoked are not shared.

All shared user metadata is removed, when the users are unshared again:

- Unpublish companies.
- Unshare contact groups.
- Change link type to NONE.

6.4 Revoke a remote system connection.

The federated connection to a remote system can be deleted and certificates revoked by an administrator with *Service access* privileges.

Revoke a system connection

Step 1: Open *System* → *Bridges*.

Step 2: Tap *Delete* to remove a system connection and revoke certificates.

Step 3: Confirm the warning.

The connection to the remote system can only be restored by establishing a new connection [Establish a server federation 6.1].

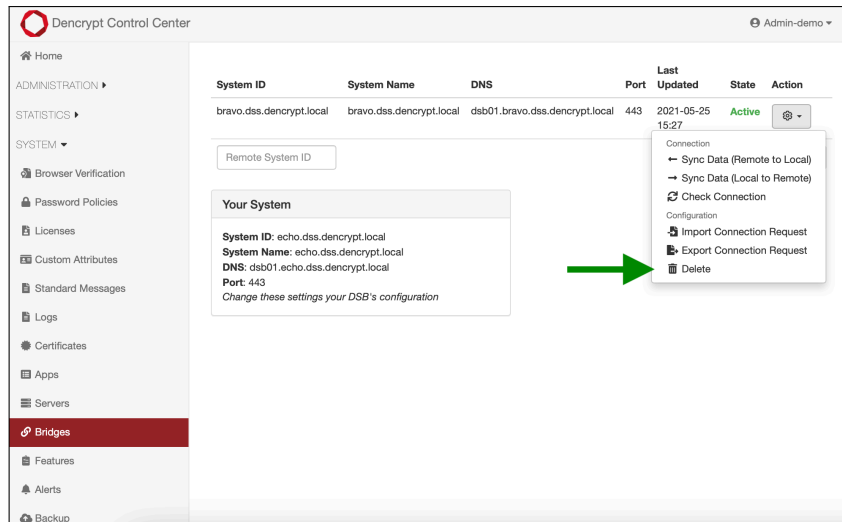


Figure 16: Revoke a remote connection.

7 Functionality in operational mode

This section contains step-by-step instructions for the functionalities available from the Dencrypt Control Center in operational mode.

7.1 Error message handling

Operating the Dencrypt Control Center (DCC) may, in some cases, produce an error as shown on Figure 17.

If an error occurs, try refreshing the web page and performing the action again. If the error persists, please take the following steps:

Error message handling.

Step 1: Tap on the exclamation mark to display the technical details of the error.

Step 2: Take a screenshot or copy the error message.

Step 3: Describe how the error was triggered e.g. a list of steps to reproduce.

Step 4: Inform the local administrator.

Certain actions may generate a warning and require additional confirmation before proceeding.

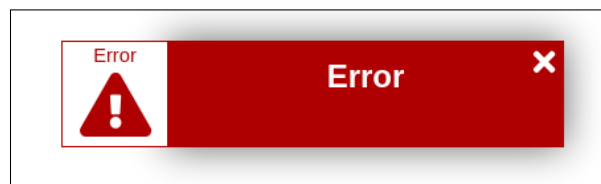


Figure 17: Error indication.

Example of how to handle an error:

Error message handling.

Step 1: An error occurred when adding a new group. Tap the Error shown at Figure 18

Step 2: Copy the error message shown at Figure 19

Step 3: Description of how the error occurred:

- Tapped on Groups-tab.
- Selected 'My Company'.
- Tapped the button to add a new group.
- Wrote 'All' in the text field for the name of the group.
- Pressed the save button.
- About 5 seconds after the error occurred.
- Refreshed the page and tried again with the same error.

Step 4: Send the error message and description to your local administrator.

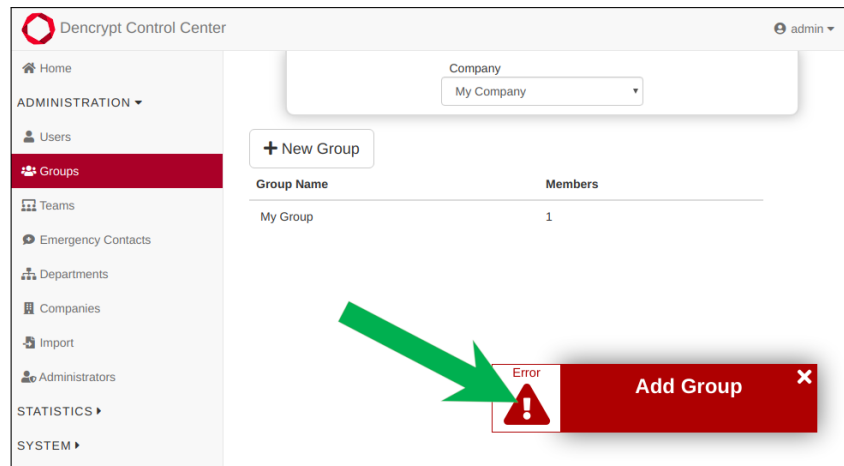


Figure 18: Where to click to show error details.

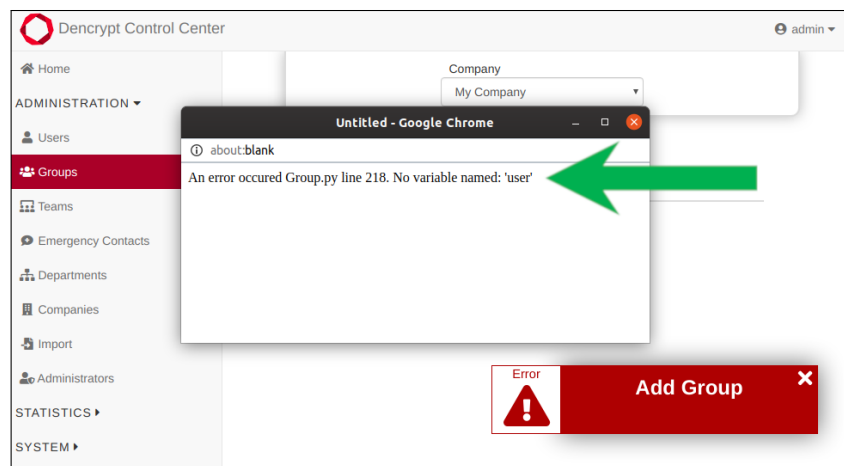


Figure 19: Message to copy for your administrator.

7.2 Login

A login is required to access the functionality of the Dencrypt Control Center (DCC). The webpage address is available from the system administrator. The login screen is presented to enter the user name and password.

If the administrator logs in for the first time, he/she is asked to change the password [Password policy 7.22]. After a successful login, the administrator is directed to the *Home* screen.

The administrator is automatically logged out after 120 minutes of inactivity.

Any administrator shall always be aware of the security instruction for accessing and operating the Dencrypt Control Center [Security instructions 2].

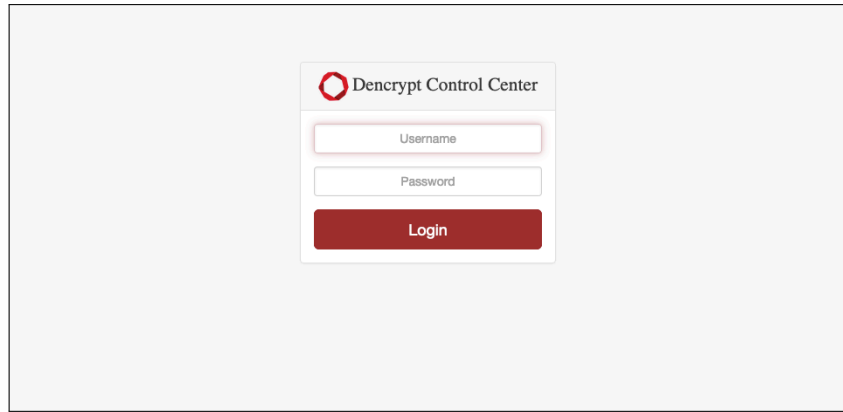


Figure 20: Login screen.

7.3 Home screen

The *Home screen* provides access to system functionality and also provides a dashboard with the operational status of the server components. The status updates every 30 seconds.

It is always possible to return the *Home screen* by tapping *Dencrypt Control Center* in the upper-left corner.

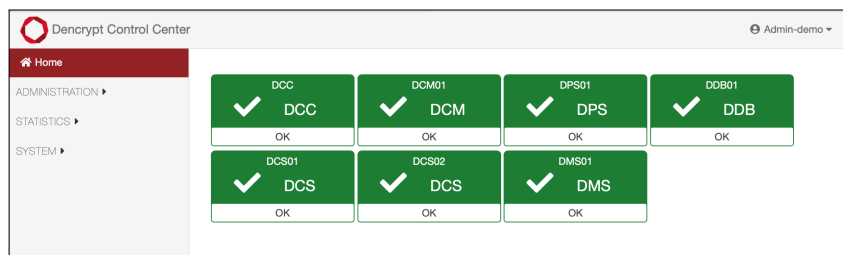


Figure 21: Home screen.

7.4 Verify version number

Verify version number

Step 1: Select the *profile menu* in the upper-right corner.

Step 2: The version number provided is the last item on the list.

Outputs:

- Version number for the Dencrypt Control Center

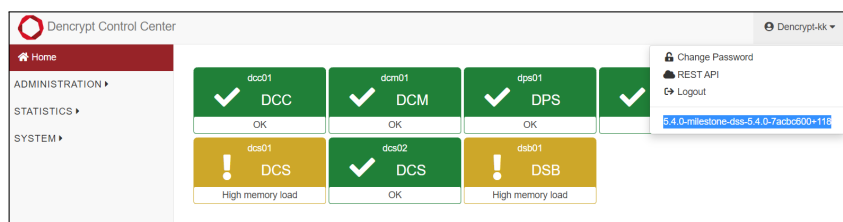


Figure 22: Verify version number.

7.5 Change Password

Change password

Step 1: Open the user profile in the top bar and select *Change Password*.

Step 2: Enter the current password and the new password twice [Password Policy 2.11].

Step 3: Tap *Change Password*.

Parameters:

Current password Enter the current password.

New password Enter the new password.

Outputs:

- The password is changed.

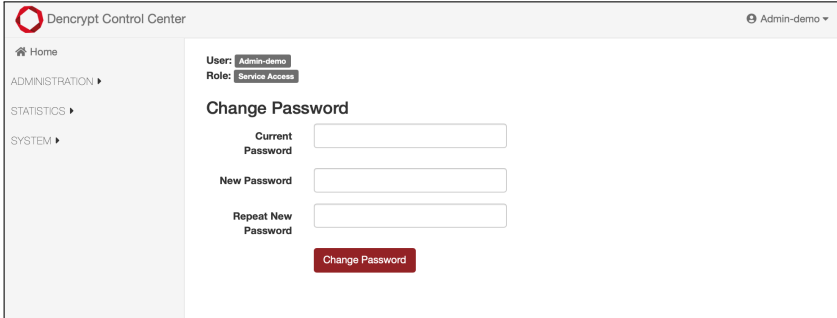


Figure 23: Change password.

7.6 Users

The *Users* page is used for managing end-users. A *User admin* only has access to the end-users of the allocated companies.

7.6.1 Display a list of users

Display a list of users

Step 1: Open on *Administration* → *Users*.

Step 2: Select the relevant company from the *Company* drop-down menu.

Step 3: Manage the columns to display from the edit menu on the right side.

Step 4: Apply search to locate specific users. The search is performed within all the visible columns.

Step 5: Sort the list by tapping any column headings.

Step 6: Select the number of users to display per page.

Parameters:

Company Specifies the company.

Outputs:

- A list of users according to the search and sort options.
- Displayed data according to the selected columns.

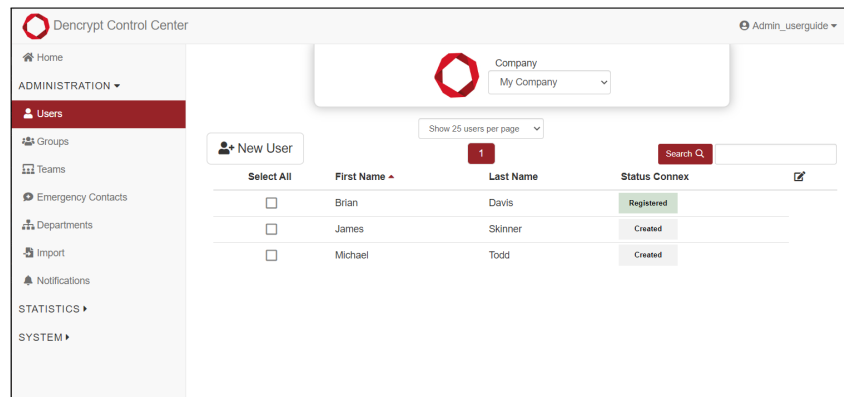


Figure 24: Frontpage for User administration.

7.6.2 Create a new user**Create new user**

Step 1: Select *New User*.

Step 2: Complete the form with title, name and department as it shall appear in the phonebook.

Step 3: Add the email address and/or phone number for provisioning.

Step 4: Allocate the user to the relevant *Groups*. A preview of the phonebook is displayed.

Step 5: Tap *Create User*. Opens the invitation window for provisioning.

Parameters:

<i>First and last name</i>	Name of the user as it appears in the phonebook.
<i>Email address</i>	Email address for receiving the invitation email for provisioning.
<i>Phone number</i>	Phone number for receiving the invitation SMS for provisioning (if SMS provisioning is enabled by the same system). The flag indicates the country code.
<i>Company</i>	(Prefilled) Used for grouping users in the phonebook.
<i>Department</i>	Used for subgrouping users within a company.
<i>Title</i>	The title of the user as it appears in the phonebook.
<i>Image</i>	Loads an avatar image. If left blank, the company logo is applied.
<i>Groups</i>	The possible contact groups to allocate membership of. See [Phonebook 3] for how to generate contact groups and individual phonebooks.

Outputs:

- The user created in the system, but not provisioned.

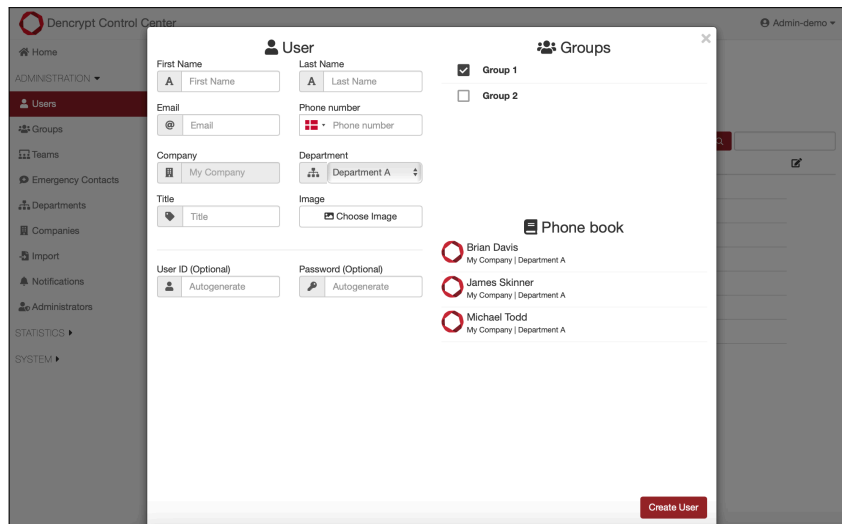


Figure 25: Create a new user.

7.6.3 Display user details

Display user details

Step 1: Select the user from the list and open *Info*:

Step 2: Displayed information:

User ID	Unique identifier
Created	Timestamp for user creation
Last revoked	Timestamp for the last revocation
Displayed	Preview user details as they appear in the phonebook
Image	The applied avatar image.
Status	Registration status
Last connected	Timestamp for last successful connection to the server system
Last invited	Timestamp for the last invitation

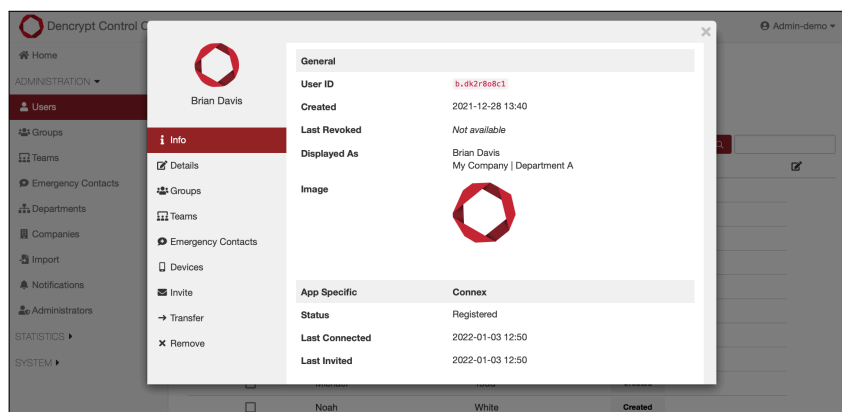


Figure 26: User details.

7.6.4 Edit user details

Modify user details

Step 1: Select the user from the list and open *Details*.

Step 2: Fill out the form and tap *Save*.

Step 3: To bulk edit multiple users: 1) enable *Bulk selection* column; 2) Select users and Tap *Details*.

Parameters:

<i>First and last name</i>	Name of the user as it appears in the phonebook.
<i>Email address</i>	Email address for receiving the invitation email for provisioning.
<i>Phone number</i>	Phone number for receiving the invitation SMS for provisioning (if SMS provisioning is enabled by the same system). The flag indicates the country code.
<i>Company</i>	(Prefilled) Used for grouping users in the phonebook.
<i>Department</i>	Used for subgrouping users within a company.
<i>Title</i>	The title of the user at it appears in the phonebook.
<i>Image</i>	Loads an avatar image. If left blank, the company logo is applied.
<i>Groups</i>	The possible contact groups to allocate membership of. See [Phonebook 3] for how to generate contact groups and individual phonebooks.

Outputs:

- The user details are modified.

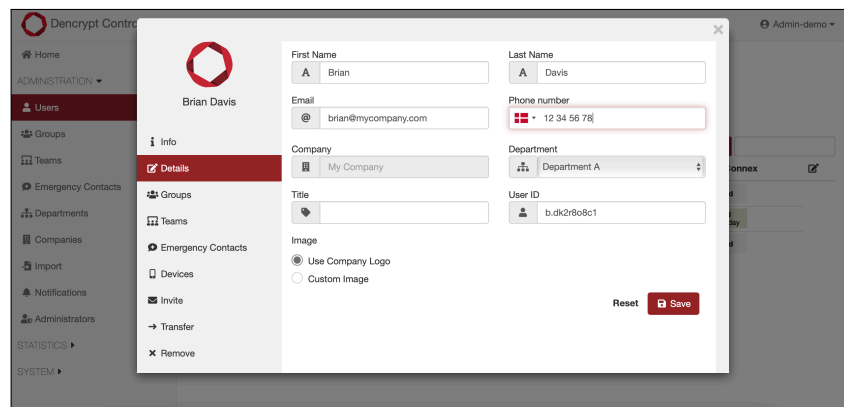


Figure 27: Edit user details.

7.6.5 Edit allocation to contact groups

Edit allocation to contact groups.

Step 1: Select the user and open *Groups* or use *Bulk selection* to allocate multiple users.

Step 2: Check the contact groups to allocate the user to the group. Remove the checkmark to remove an allocation.

Step 3: Verify the phonebook preview.

Step 4: Tap *Save*.

Step 5: (Bulk selection) Toggle the check box to: 1) to allocate all selected users (green checkmark), 2) to remove all selected users from the group (red cross mark), see Figure 29.

Outputs:

- Updated allocation to contact groups.

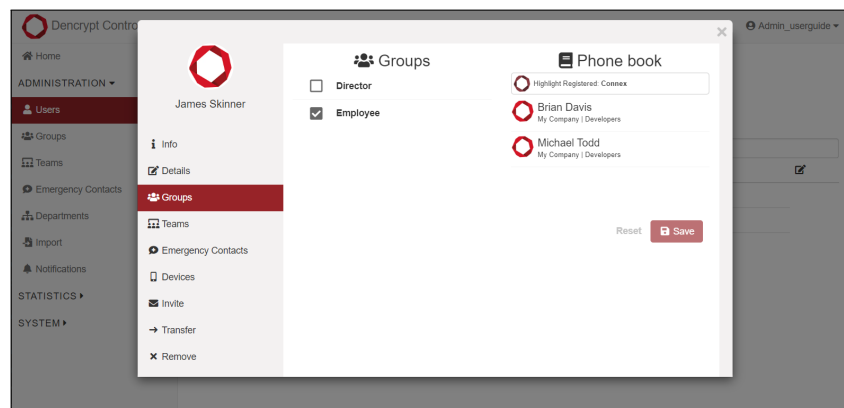


Figure 28: Edit allocation to contact groups.

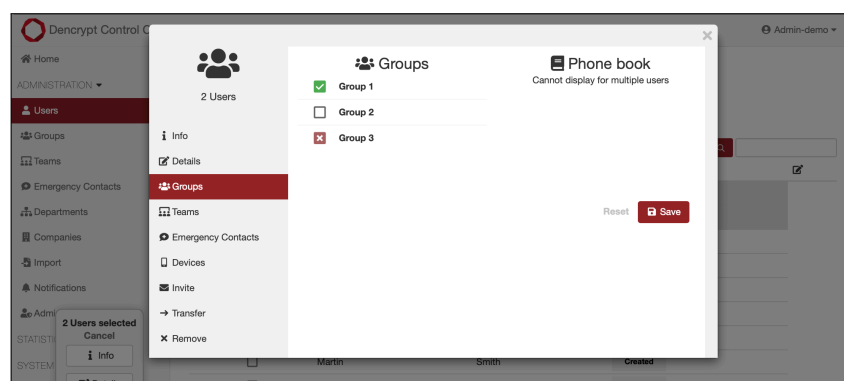


Figure 29: Edit allocation to contact groups for multiple users.

7.6.6 Allocate users to teams

Refer to [Teams 4] for a description of *Teams*.

Allocate users to teams

- Step 1: Select the user and open *Teams* or use *Bulk selection* to allocate multiple users.
- Step 2: Check the checkboxes next to the teams to allocate users. Select the *Team* to preview the members.
- Step 3: Tap *Save*.
- Step 4: (Bulk selection) Toggle the check box to: 1) to allocate all selected users (green checkmark), 2) to remove all selected users from the group (red cross mark), see Figure 31.
- Step 5: Select a team to display the members.

Outputs:

- Update allocation to teams.
- Display team members.

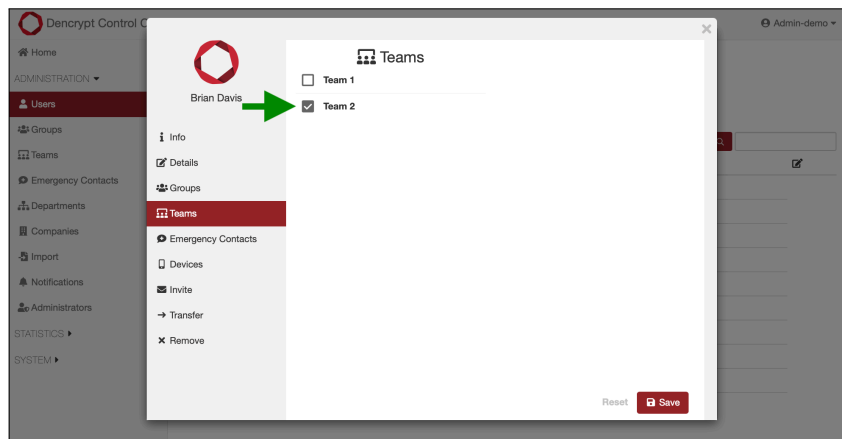


Figure 30: Allocate users to teams.

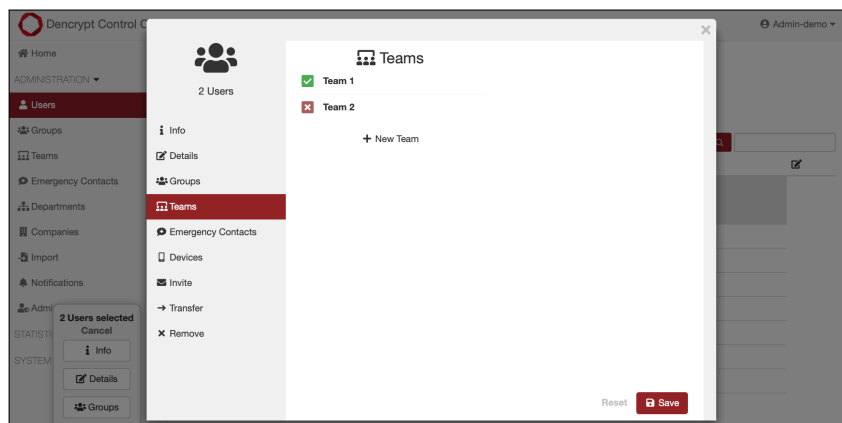


Figure 31: Edit allocation to teams for multiple users.

7.6.7 Allocate emergency lists

Refer to [Emergency contacts 5] for a description of *Emergency contacts*.

Allocate users to emergency lists HUSK MIG

Step 1: Select the user and open *Emergency contacts* or use *Bulk selection* to allocate multiple users.

Step 2: Check the checkboxes next to the emergency lists to allocate users. Select the *Emergency list* to preview the emergency contacts.

Step 3: Tap *Save*.

Step 4: (Bulk selection) Toggle the check box to: 1) to allocate all selected users (green checkmark), 2) to remove all selected users from the list (red cross mark), see Figure 33.

Outputs:

- Update allocation to emergency lists.
- Display list members.

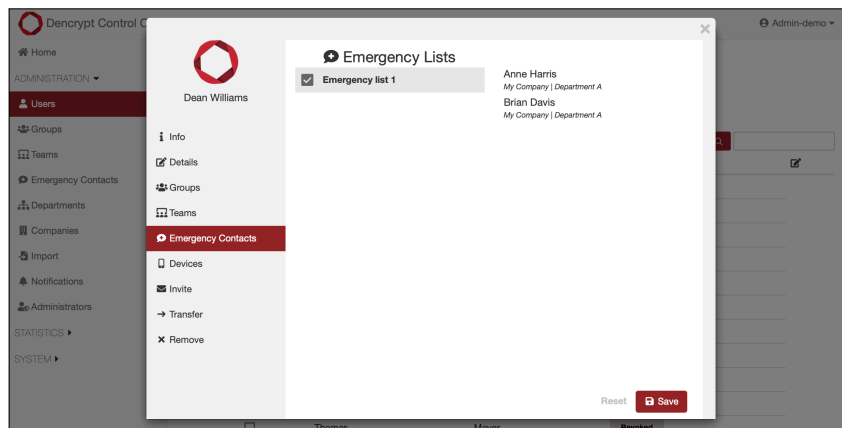


Figure 32: Allocate users to emergency lists.

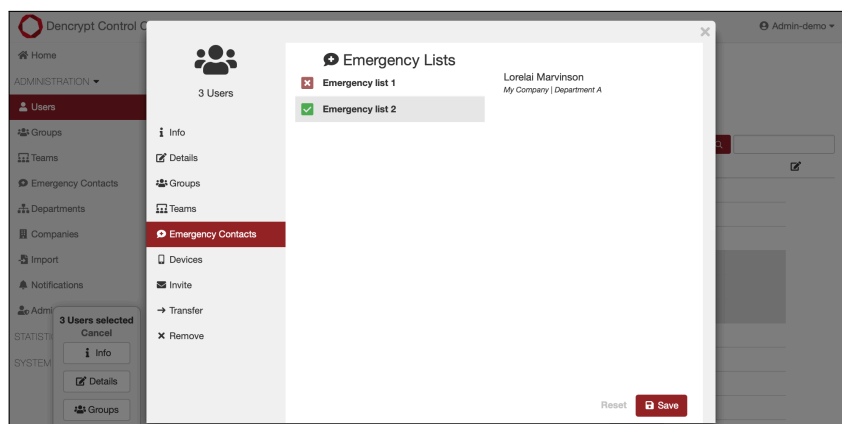


Figure 33: Edit allocation to emergency lists for multiple users.

7.6.8 Manage user devices

Display device information.

Manage user devices

Step 1: Select the user and open *Devices* or use *Bulk selection* to select multiple users.

Step 2: Select a device to view additional information.

Parameters:

Info

<i>ClientId</i>	Device specific application id.
<i>Application</i>	Application name.
<i>Device</i>	Manufacturer and device model.
<i>Operating system</i>	OS type and version.
<i>Created</i>	Timestamp for device creation in the system.
<i>Last Registration</i>	Timestamp for the last successful connection to the system.

Push tokens

<i>Certificate</i>	Certificate name for push token.
<i>Capability</i>	Related push service.
<i>Encryption</i>	Support for content encryption.

Client certificate

<i>Status</i>	Certificate status: Valid, Expired or Revoked.
<i>Serial</i>	Certificate serial number.
<i>Created</i>	Timestamp for creation.
<i>Expiry</i>	Expiry date.

Outputs:

- Display of device data.

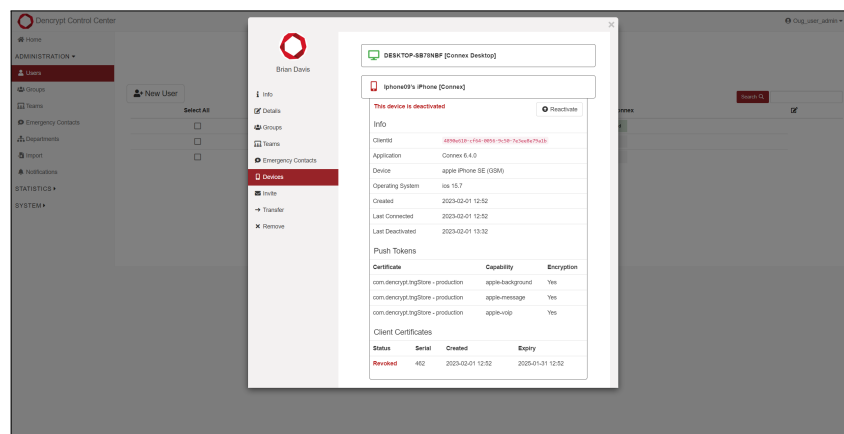


Figure 34: Manage user devices

7.6.9 Send invitation

Refer to [First time access for administrator 2.10] for details on secure provisioning.

Send invitation for provisioning

Step 1: Select the user and open *Invite* or use *Bulk selection* to invite multiple users.

Step 2: Select the application.

Step 3: Select the invitation method: *Email*, *QR Code* or *Link*.

Step 4: Tap *Invite*

Outputs:

- Submitted invitation and provisioning link to the user device.
-

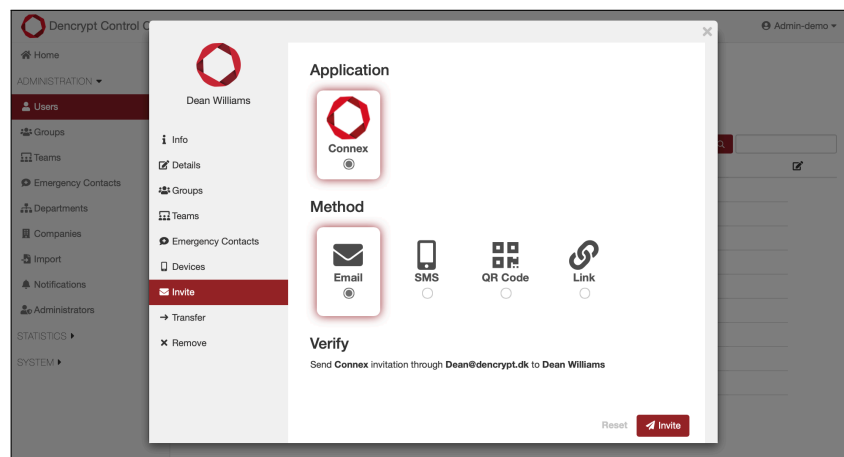


Figure 35: Send invitations for provisioning.

7.6.10 Transfer user to another company

Transfer users to another company

Step 1: Select the user and open *Transfer* or use *Bulk selection* to transfer multiple users.

Step 2: Select the target company.

Step 3: Select the target department.

Step 4: Tap *Transfer*.

Outputs:

- User transferred to the target company.
-

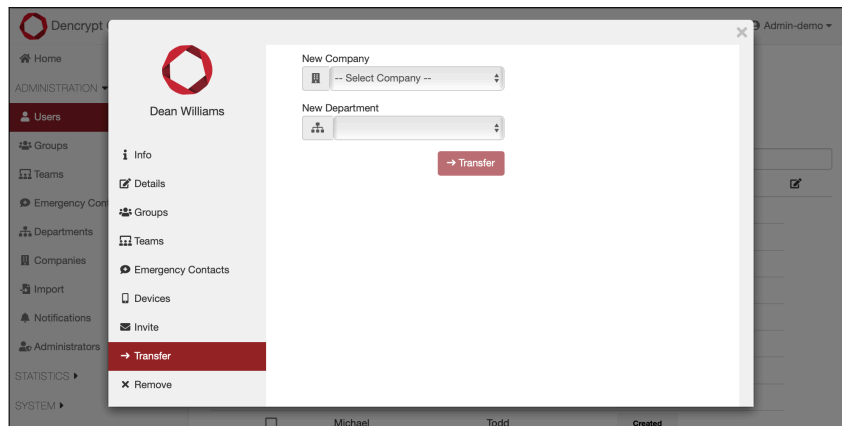


Figure 36: Transfer user to another company.

7.6.11 Remove and deactivate users

Remove/deactivate users

Step 1: Select the user and open *Remove* or use *Bulk selection* to remove/deactivate multiple users.

Step 2: Tap *Deactivate* to remove system access for all devices.

Step 3: Tap *Delete* to remove the user from the system.

Outputs:

- Deactivate: Client certificates for all devices are deactivated and the user cannot access the system.
- Delete: Client certificates for all devices are deactivated and the user account is deleted.

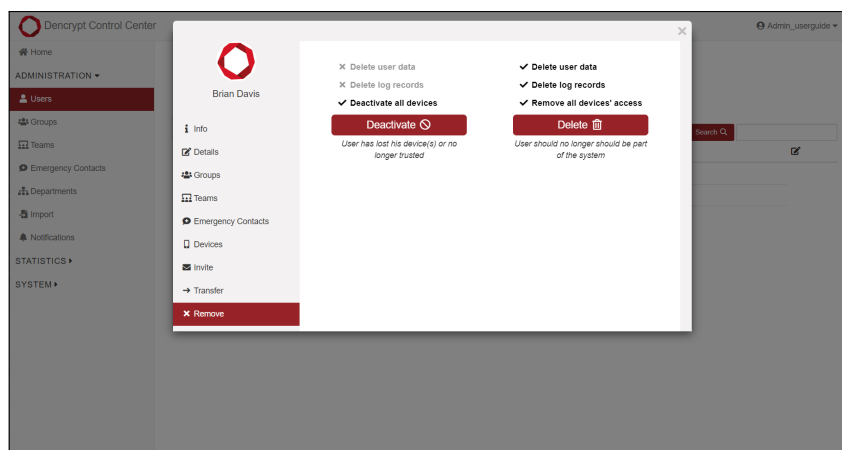


Figure 37: Remove or deactivate users.

If only one device needs to be deactivated, refer to the *Deactivate* button under *Devices* (see section 7.6.8).

7.7 Manage contact groups

Contact groups are used to generate individual phonebooks (see [Phonebook 3] for details).

Access groups frontpage

Step 1: Open *Administration* → *Groups*.

Step 2: Select the company from the dropdown menu.

Parameters:

Company Selected company

Outputs:

- List of defined contact groups within the company.
- Number of members in each group.

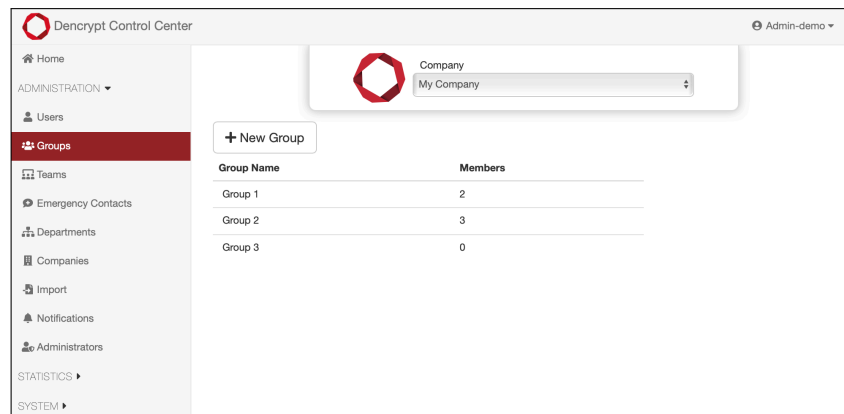


Figure 38: Frontpage for contact groups management.

7.7.1 Create a new Group

Create new contact group

Step 1: Open *Administration* → *Groups*.

Step 2: Tap *New group*

Step 3: Enter the name of the contact group

Step 4: Tap *Create Group* and open *Group* information window.

Parameters:

Name Name of the contact group.

Outputs:

- Contact group created.

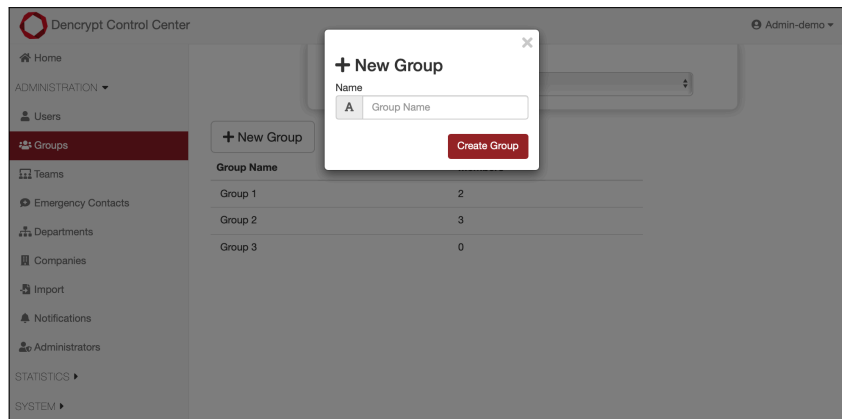


Figure 39: Create new contact group.

7.7.2 Edit and linking contact groups

Edit and linking contact groups

Step 1: Open *Administration* → *Groups*.

Step 2: Select a contact group to open the *Group info* window.

Step 3: The *Group info* window shows a list of shared and unshared companies.

Step 4: Tap *Unshared* to share a company. A list of contact groups is displayed. Selecting a contact group display its members.

Step 5: Create and modify links by toggling the Link type: NONE, BOTH, IN or OUT.

Parameters:

Name Identifier of the contact group.

Outputs:

- Updated links to other contact groups.

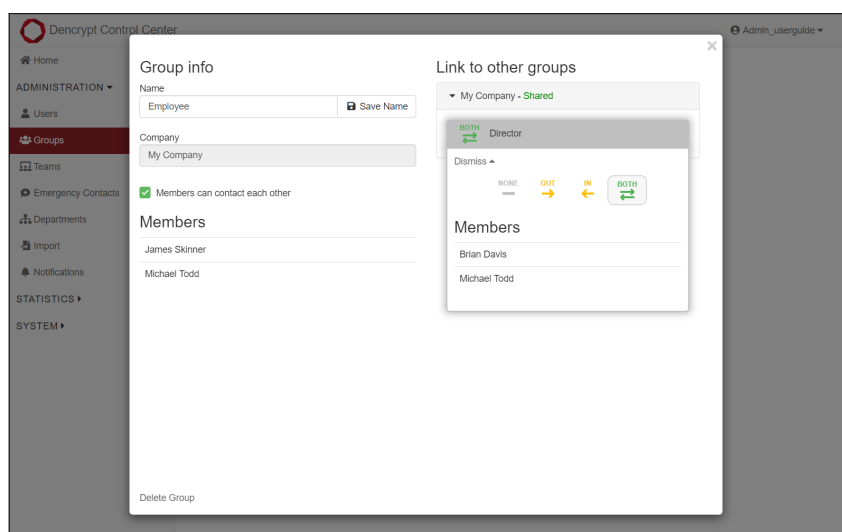


Figure 40: Edit and link contact groups.

7.8 Teams

Teams are a collection of users to form a centrally managed chat room [Teams 4].

Access Teams frontpage

Step 1: Open *Administration* → *Teams*.

Step 2: Select the company from the dropdown menu.

Parameters:

Company Selected company

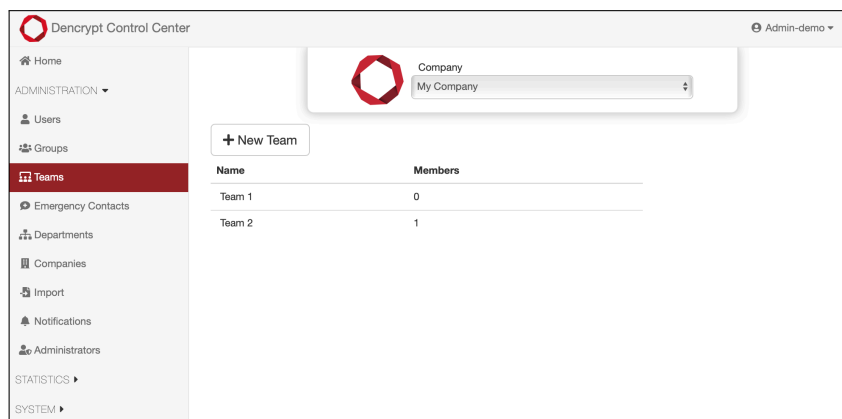


Figure 41: Frontpage for Teams

7.8.1 New Team

Create new team

Step 1: Tap on *New Team*.

Step 2: Enter the team name.

Step 3: Tap *Create Team*.

Parameters:

Name Team name. The team name will be displayed for end-users.

Outputs:

- New team created.

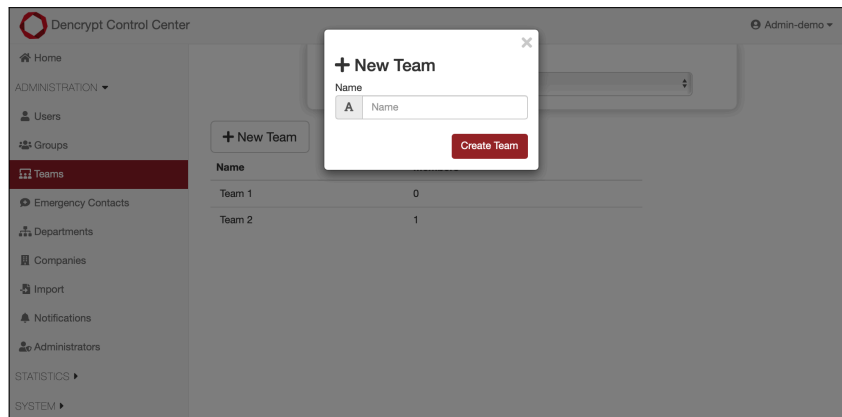


Figure 42: Create new team

7.8.2 Display and edit team details

Display and edit team details

Step 1: Select the team from the list

Step 2: Check the companies, with whom the team is shared.

Step 3: To allocate users to the team: Refer to [Allocate users to teams 7.6.6].

Step 4: To change the team name: Enter the new name and tap *Save name*

Step 5: To delete team: Tap *Delete Team* and confirm warning.

Parameters:

Name Team name

Outputs:

- Updated name of a team.

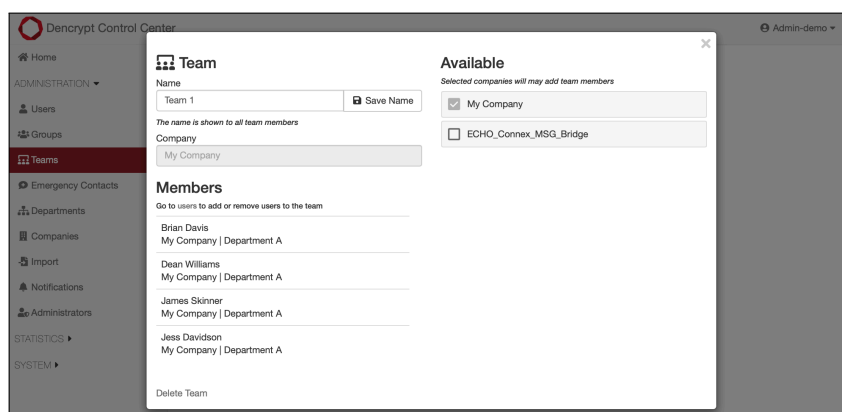


Figure 43: Display and edit team details.

7.9 Emergency contacts

Emergency lists are groups of users to be contacted in case of an emergency message sent from the Dencrypt apps [Emergency contacts 5].

Access frontpage for emergency contacts

Step 1: Open *Administration* → *Emergency Contacts*.

Step 2: Select the company from the dropdown menu.

Parameters:

Company Selected company

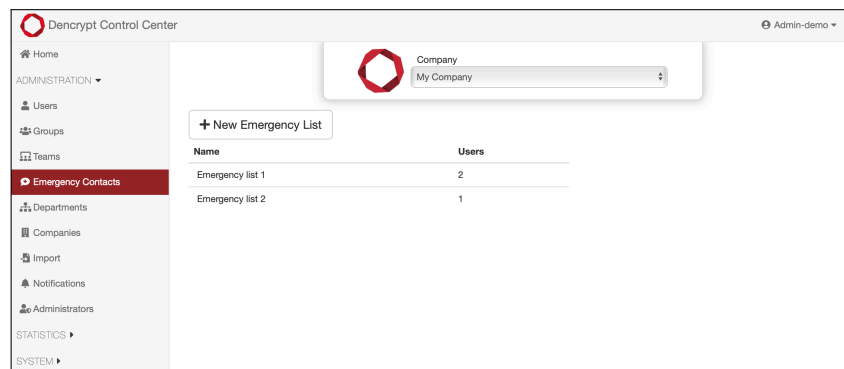


Figure 44: Acces frontpage for emergency contacts.

7.9.1 Create a new emergency list

Create new emergency list

Step 1: Select *New Emergency List*.

Step 2: Enter a name for the emergency list.

Step 3: Tap *Create List*.

Parameters:

Name Name of the emergency list. The name is only visible to administrators.

Outputs:

- New emergency list created.

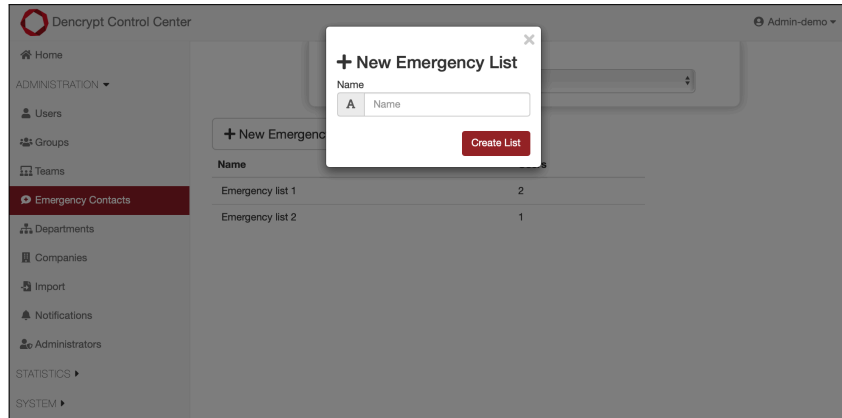


Figure 45: Create new emergency list.

7.9.2 Allocate users to emergency list

Allocate users to an emergency list

-
- Step 1: Select the emergency list.
- Step 2: Check the companies, with whom the emergency list is shared.
- Step 3: Add members to the emergency list by entering their name to the *Contacts* field. Suggestions are provided while typing.
- Step 4: Tap the cross-icon to remove members and confirm the warning.
- Step 5: To change the list name: Enter the new name and tap *Save name*.
- Step 6: To delete the list: Tap *Delete Emergency list* and confirm warning.
-

Parameters:

- Name* Identifier for emergency lists.
- Contacts* Users allocated to the list.
-

Outputs:

- Updated user allocations to an emergency list.
-

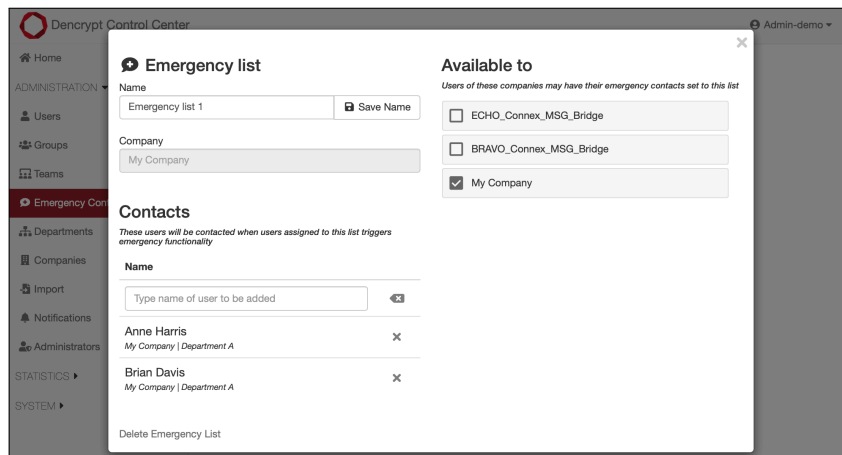


Figure 46: Allocate users to emergency lists.

7.10 Departments

Departments are labels to categorize users within a company.

Access frontpage for Departments

Step 1: Open *Administration* → *Departments*.

Step 2: Select the company from the dropdown menu.

Parameters:

Company Selected company

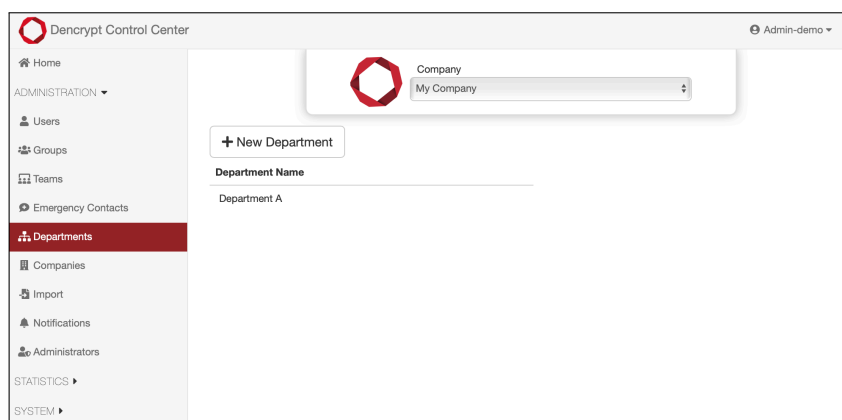


Figure 47: Frontpage for departments management.

7.10.1 Create new department

Create new department

Step 1: Select on *New Department*.

Step 2: Enter the name of the department.

Step 3: Tap *Create Department*.

Parameters:

Name Name of the department. The department's name is visible in users' phonebooks.

Outputs:

- New department created.
-

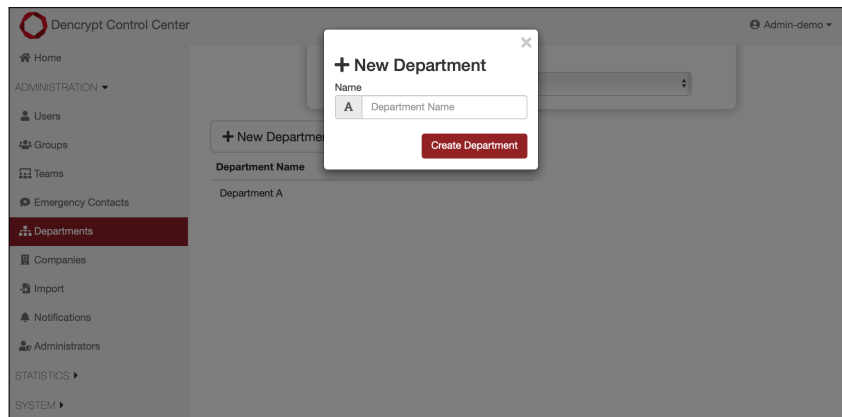


Figure 48: Create new department.

7.10.2 Edit department name

Edit department name

Step 1: Select the department from the list.

Step 2: To change the name: Enter the new name and tap *Save*.

Step 3: To delete department: Tap *Delete Department* and confirm warning. Only possible, when the department is not used by any users.

Parameters:

Name New name of the department.

Outputs:

- Modified or deleted department.

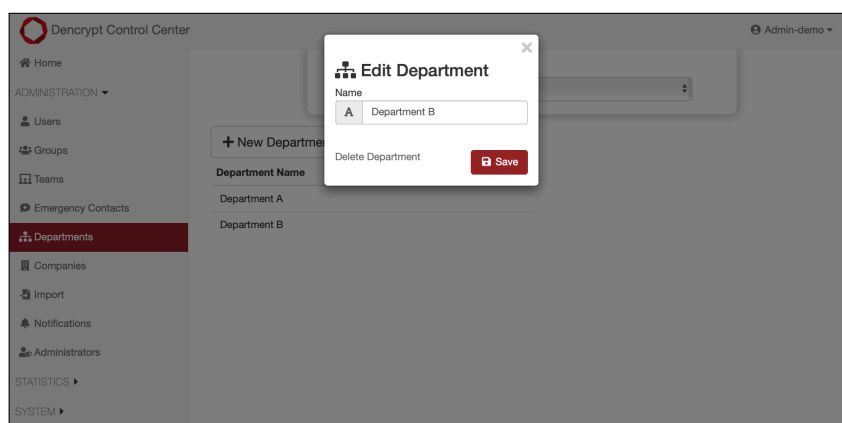


Figure 49: Edit department name.

7.11 Companies

Companies are used to contain users, departments and contact groups. A *User admin* can only manage the companies for which he/she has been allocated.

Access frontpage for company management

Step 1: Open *Administration* → *Companies*.

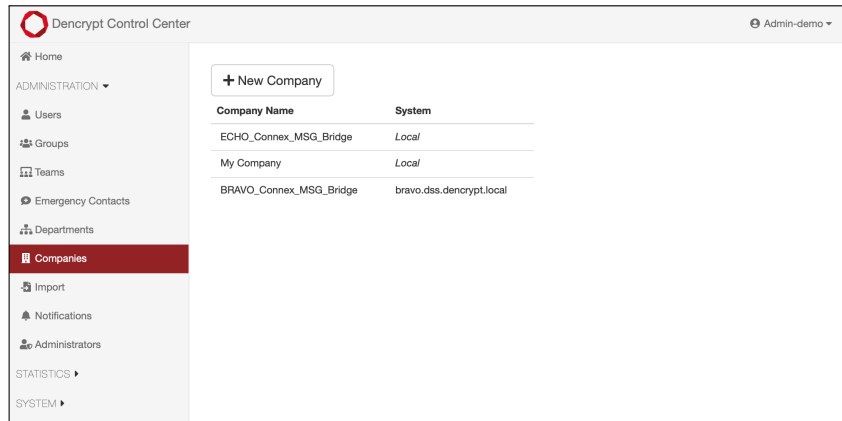


Figure 50: Access frontpage for Company management

7.11.1 Create new company

Create new company

Step 1: Select *New Company*.

Step 2: Enter a name

Step 3: Press *Create Company* to open window for editing details.

Parameters:

Name Name of the company. The company name is visible in the users' phonebooks.

Outputs:

- New company created.

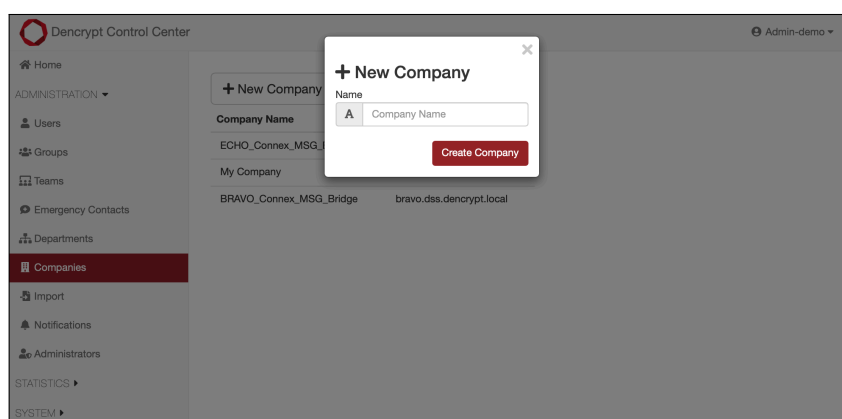


Figure 51: Create new company.

7.11.2 Edit company details

Edit the company details and relations to other systems.

Edit company details

Step 1: Select the company from the list

Step 2: To change company name: Enter the new name.

Step 3: To change logo-file: Tap *New image* to upload image file.

Step 4: To delete company: Tap *Delete Company*. Confirm the warning. If the company is used by any users, departments or groups, another warning will appear. Confirm by writing *DELETE*.

Step 5: Tap *Save*.

Parameters:

Name New name of the company

Logo Image file to display as default avatar

Outputs:

- Modified or deleted company.

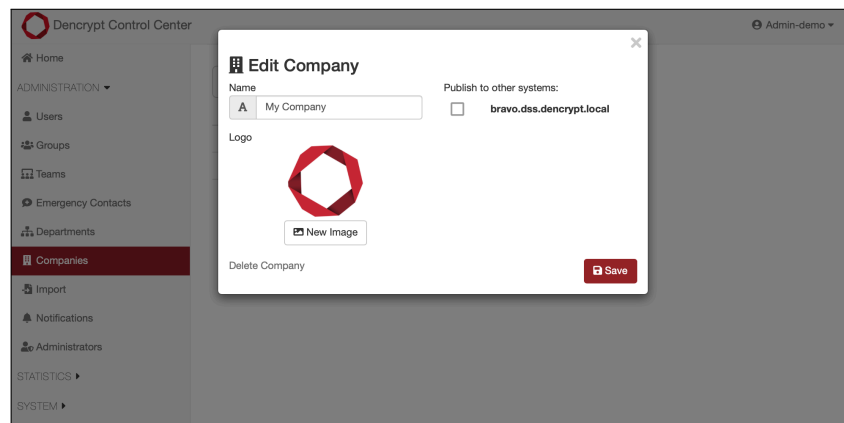


Figure 52: Edit company details.

7.12 Import users

Bulk import of users is possible by uploading an Excel import file.

Import users from Excel sheet

Step 1: Open *Administration* → *Import*.

Step 2: Download template file.

Step 3: Tap *Select Excel File* to upload an Excel import file.

Step 4: Review the changes from the preview of users, companies, departments and groups.

Step 5: Tap *Confirm*.

Step 6: Tap *Continue* to complete the import or *Import Another File*.

Parameters:

Excel import file Must be formatted according to the template file.

Outputs:

- Imported users, companies, departments and groups.
-

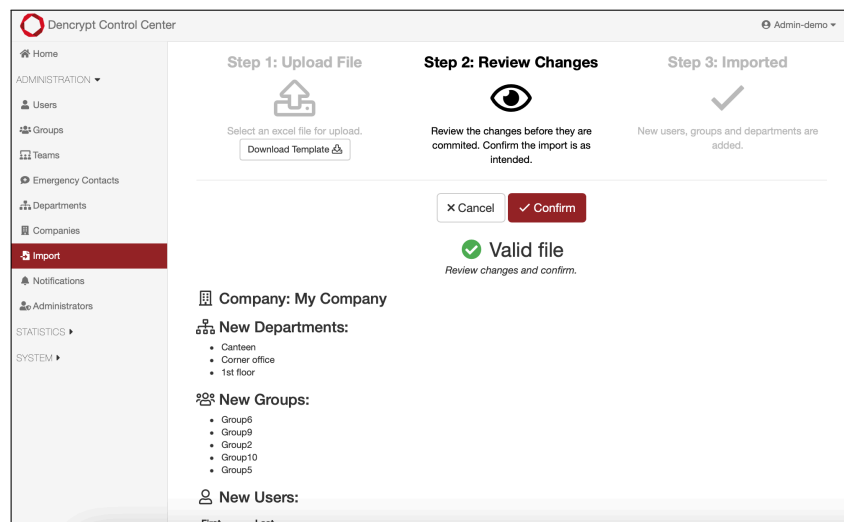


Figure 53: Import users

7.13 Administrators

Administrators are the user of the Dencrypt Control Center with the privileges determined by their roles [Roles and Permissions 2.13].

Access frontpage for administrator management

Step 1: Open *Administration* → *Administrators*.

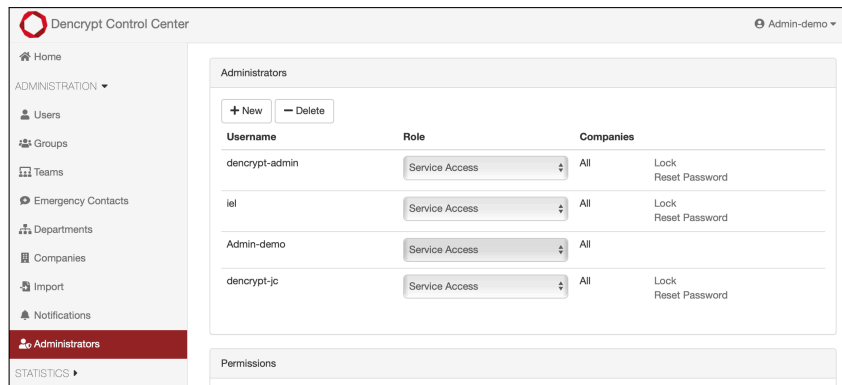


Figure 54: Frontpage for administrator management.

7.13.1 Create administrator account

Create new administrator account

Step 1: Tap on + *New*.

Step 2: Enter name, one-time password and role

Step 3: Tap *Create Administrator*.

Parameters:

Username Unique user name

Password First-time password. It will be changed by the new administrator at the first login.

Role Specify the administrator role [Roles and Permissions 2.13].

Outputs:

- Administrator account created with login credentials.

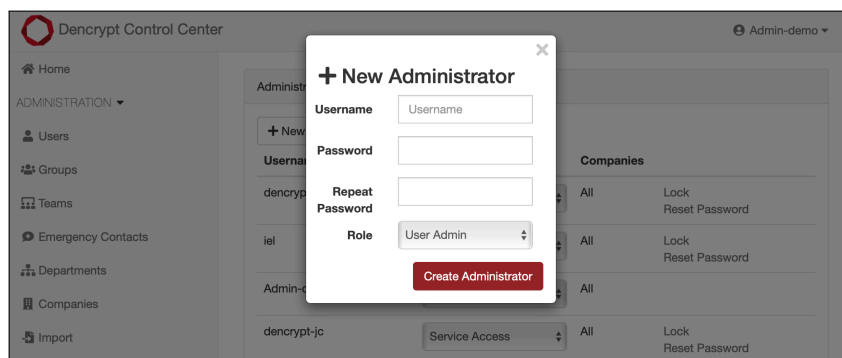


Figure 55: Create new administrator account.

7.13.2 Delete administrator accounts

Delete administrators

Step 1: Tap on – *Delete*.

Step 2: Select the administrators to be deleted.

Step 3: Press *Delete Administrators* and confirm the warning.

Outputs:

- Administrator account(s) deleted.
-

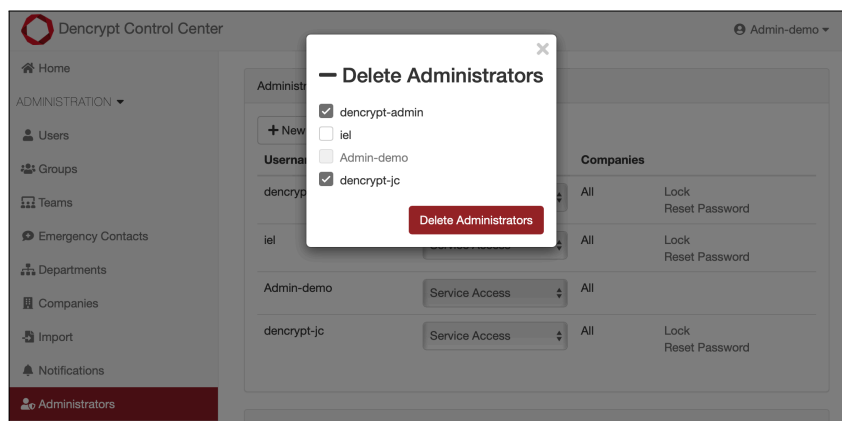


Figure 56: Delete administrator accounts.

7.13.3 Change role

Change administrator role

Step 1: Select the administrator from the list.

Step 2: Select the new role from the dropdown menu.

Parameters:

Role New administrator role [Roles and Permissions 2.13].

Outputs:

- Administrator privileges changed.
-

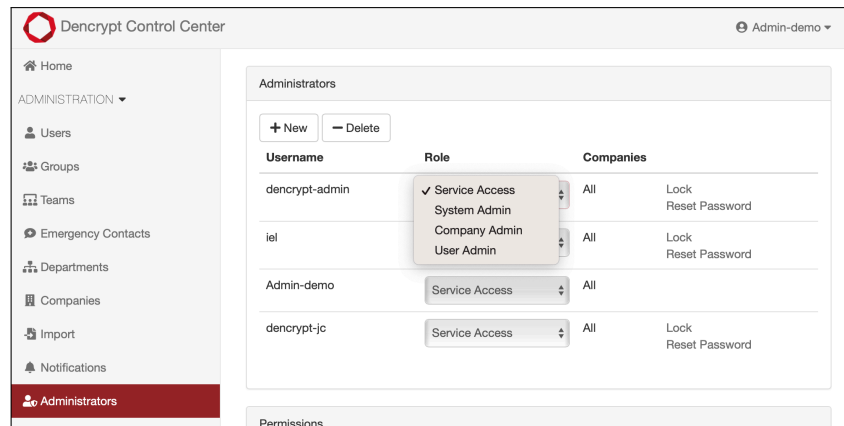


Figure 57: Change administrator role.

7.13.4 Apply company access for User admin

Defines the companies, which an administrator with *User admin* privileges can access.

Apply company access

Step 1: Select the administrator in the list.

Step 2: Tap *Edit* in the Companies column to open a list of available companies.

Step 3: Select one or more companies.

Outputs:

- The administrator is granted access to managing users within the selected companies.

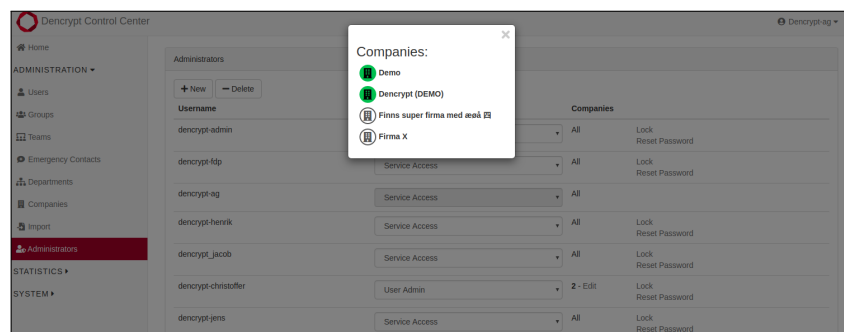


Figure 58: Apply company access.

7.13.5 Lock and password reset

An account can be locked preventing the administrator from accessing the Dencrypt Control Center.

Lock an administrator account

Step 1: Select the administrator from the list

Step 2: Tap *Lock* to lock the account. Confirm the warning.

Step 3: Tap *Unlocked* to restore access. Confirm the warning.

Outputs:

- Administrator accounts are locked/unlocked.

Change administrator password

Step 1: Select the administrator from the list

Step 2: Tap *Reset password* to create a new one-time password.

Step 3: Enter the new password twice.

Step 4: Tap *Reset Password*

Outputs:

- Password changed.

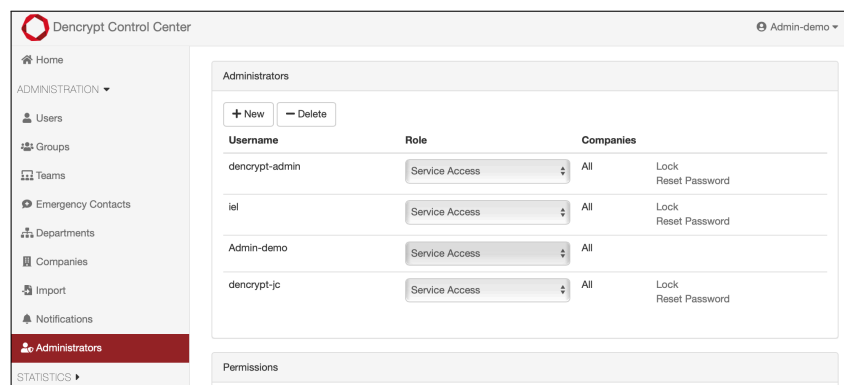


Figure 59: Lock account and reset password.

7.14 Calls statistics

Call statistics per system or per company are collected to monitor system usage.

Access call statistics

Step 1: Open *Statistics* → *Calls*.

Step 2: Select the company (or all companies) from the drop-down menu to display the statistics.

Step 3: Select the time period from the drop-down menu.

Step 4: Select a bar to display statistics for the current day.

Step 5: Tap *Show details* to display statistics per status codes.

Parameters:

- Company** Shows statistics for the selected company. *All companies* is also an option.
- Time period** Select the observation period: *Show all calls*, *Show calls for a week*, *Show calls for a month* or *Show calls for a year*.

Outputs:

- A bar graph displays the daily calls in the observed period indicating the number of *Successful calls*, *Unavailable calls* and calls terminating with an error condition.

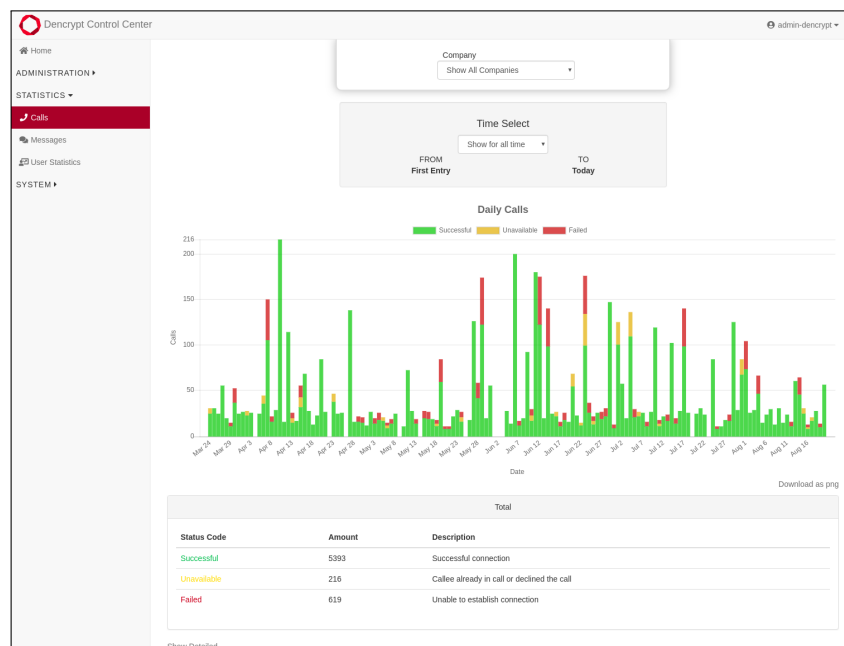


Figure 60: Call statistics

7.15 Message statistics

Message statistics per system or per company are collected to monitor system usage.

Access message statistics

- Step 1: Open *Statistics* → *Messages*.
- Step 2: Select the company (or all companies) from the drop-down menu to display the statistics.
- Step 3: Select the time period from the drop-down menu.
- Step 4: Select a bar to display statistics for the current day.
- Step 5: Tap *Show details* to display statistics per status codes.

Parameters:

- Company** Shows statistics for the selected company. *All companies* is also an option.
- Time period** Select the observation period: *Show all messages*, *Show messages for a week*, *Show messages for a month* or *Show messages for a year*.

Outputs:

- A bar graph displays the daily messages exchanged in the observed period.

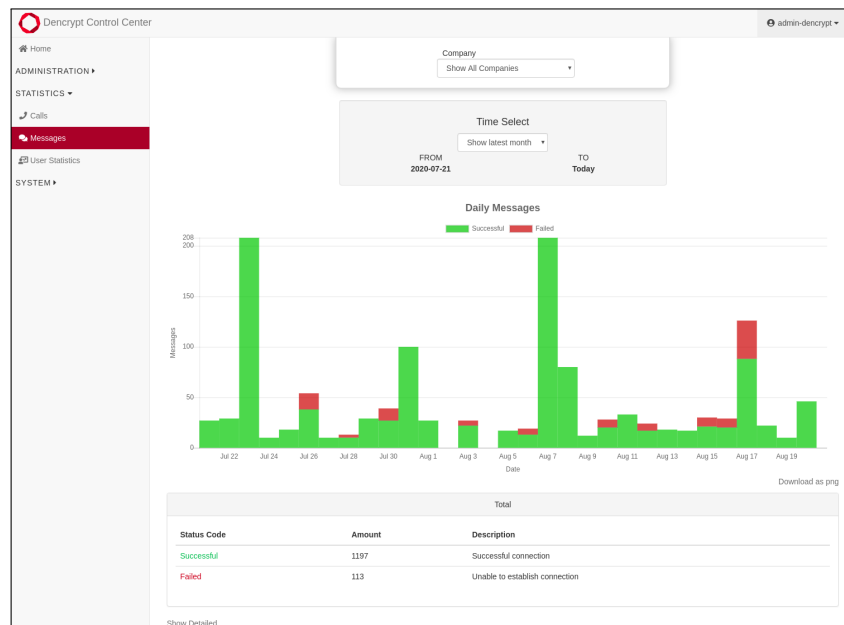


Figure 61: Message statistics

7.15.1 Access user statistics**Access user statistics**

Step 1: Open *Statistics* → *User Statistics*.

Step 2: Select *Show as table* to toggle between a table view and a graphical view.

Outputs:

- Number of total users and users per company.
- Number of users with status: *Registered*, *Invited*, *Revoked*, *Created*.

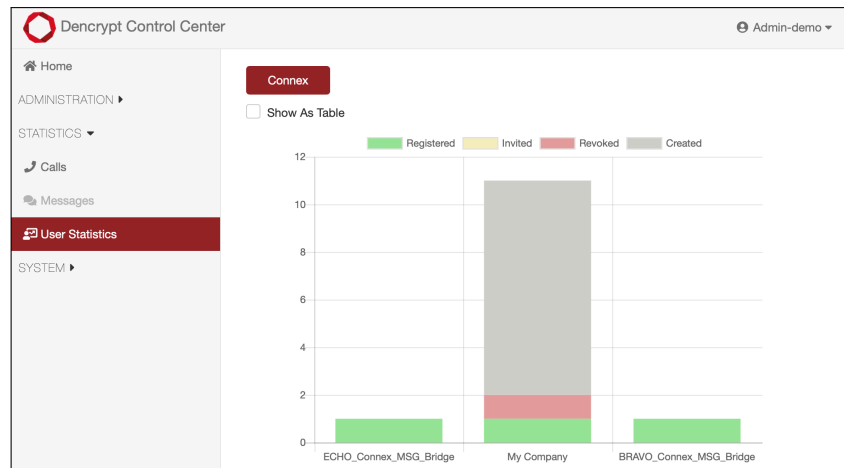


Figure 62: User statistics

7.15.2 Download user statistics

Download user statistics as .csv

Step 1: Open *Statistics* → *User Statistics*.

Step 2: Select companies and metadata

Step 3: Tap *Download as CSV*

Parameters:

Companies Companies from which to include data.

Data Statistics to include:

Per user: *UserID, Name, Email, Phone number, Company, Department, Title, Created*

Per app: *registration status, Number of calls/messaging, Time stamps for last Connection, Last invitation, last revocation*

Outputs:

- Downloaded file (.csv) containing the selected data.

Report Statistics of Users


Companies	Data	Format
<input type="checkbox"/> ECHO_Connex_MSG_Bridge	<input type="checkbox"/> UserID	Download as CSV 
<input checked="" type="checkbox"/> My Company	<input checked="" type="checkbox"/> Name	
<input type="checkbox"/> BRAVO_Connex_MSG_Bridge	<input type="checkbox"/> Email	
	<input type="checkbox"/> Phone number	
	<input type="checkbox"/> Company	
	<input type="checkbox"/> Department	
	<input type="checkbox"/> Title	
	<input type="checkbox"/> Created	
	<input type="checkbox"/> Calls	
	<input type="checkbox"/> Messages	
	Connex	
	<input type="checkbox"/> Status	
	<input type="checkbox"/> Last Connected	
	<input type="checkbox"/> Last Invited	
	<input type="checkbox"/> Last Revoked	

Figure 63: Download user statistics

7.16 Download browser certificate

Download the root certificate to be installed in the browser for server verification.

Download browser certificate

Step 1: Open *System* → *Browser Verification*.

Step 2: Tap *Download As File*.

Step 3: Follow steps in [Install the browser certificate 2.12] to install the certificate.

Outputs:

- Downloaded *root-certificate.crt* for browser installation.
-

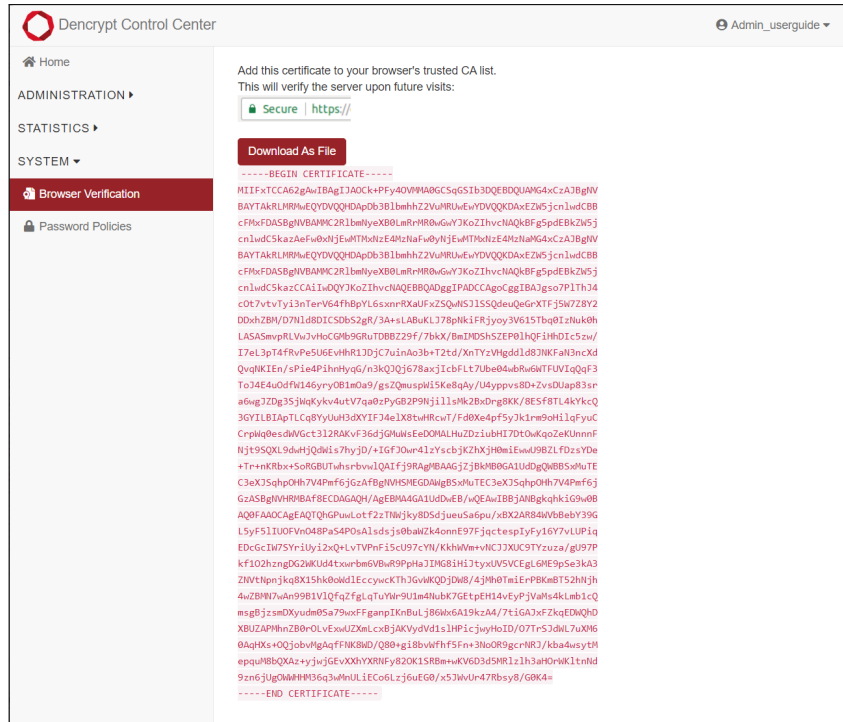


Figure 64: Download browser certificate.

7.17 License management

Display license status

Step 1: Open *System* → *Licenses*.

Outputs:

- Display: *Total number of licenses, Unused licenses and expiry time.*
- Display: *Created users per company and maximum users allowed per company (if set)*

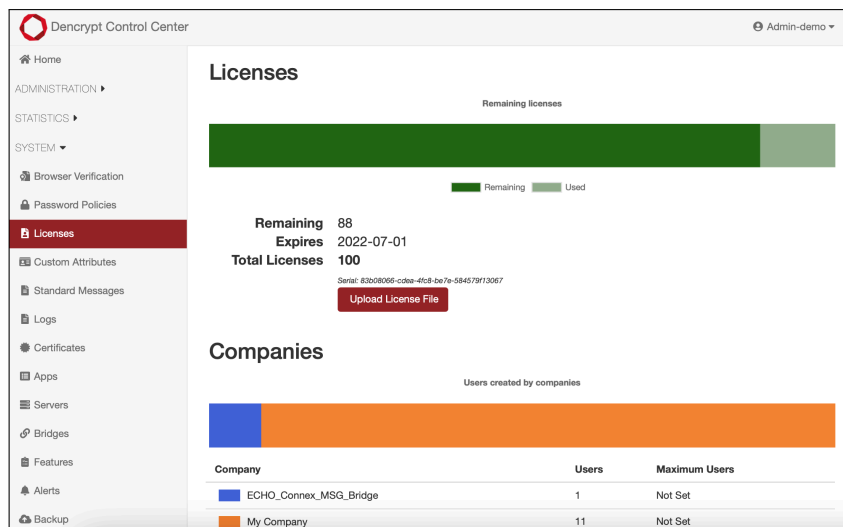


Figure 65: License overview.

7.17.1 Upload license file

Licenses are renewed or expanded by installing a license file received from Dencrypt.

Upload license file

Step 1: Tap *Upload License File*

Step 2: Select and open the license file on your local computer.

Parameters:

License file License file received by Dencrypt.

Outputs:

- Licenses updated with the expiry date.
- Licenses updated with an upper limit of users.

7.17.2 Set user limit per company

Set user limit per company.

Step 1: Select the company from the list.

Step 2: Tap the number or "Not set" in the *Maximum users* column.

Step 3: Specify the maximum number of users and select *Save*.

Parameters:

Max. users Maximum number of users allowed per company. When left blank an unlimited amount of users is allowed.

Outputs:

- Updated amount of maximum users per company.

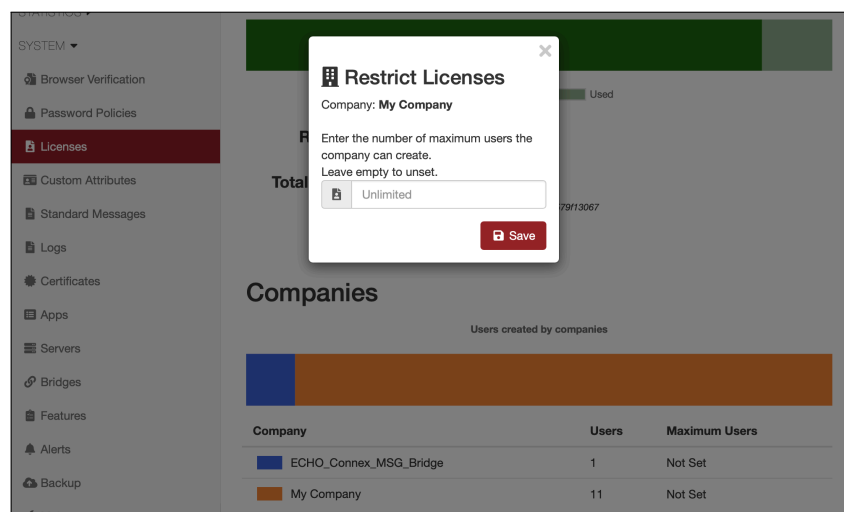


Figure 66: Set user limit per company

7.18 Apps

The *Apps* section lists the Dencrypt app variants configured for the system. New app definitions using JSON format can be uploaded.

App variation concerns: app name, app icon, supported OS and appearance of activation invitations.

List configured apps

Step 1: Open *System* → *Apps*.

7.18.1 Apps Definitions

Download definition file

Step 1: Tap *Download Current* on the top of the page.

Outputs:

- App variants file downloaded. The file can be modified and uploaded to define new app variants.

Upload definition file

Step 1: Tap *Upload App Variants File* on the top of the page.

Step 2: Select an app variants file (.json).

Parameters:

Filename Filename for definition file.

Outputs:

- Updated list of supported apps.

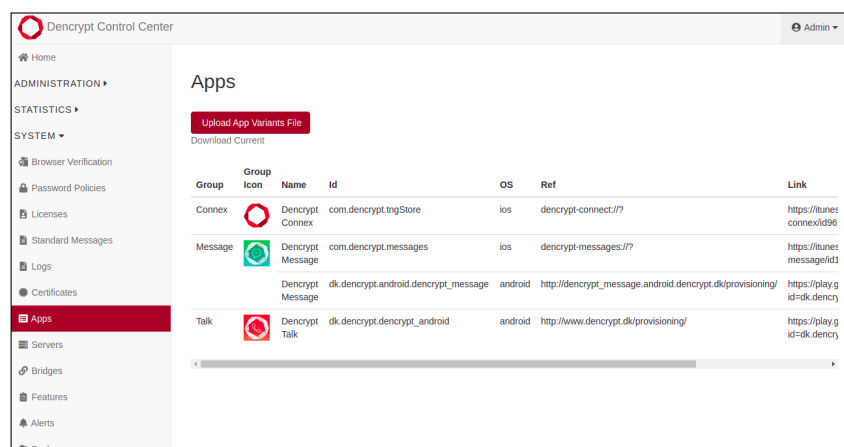


Figure 67: Apps Management.

7.19 Standard Messages

Standard messages are pre-defined messages defined by the system administration and available for end-users for quick messaging.

Access frontpage for standard messages

Step 1: Open *System* → *Standard Messages*.

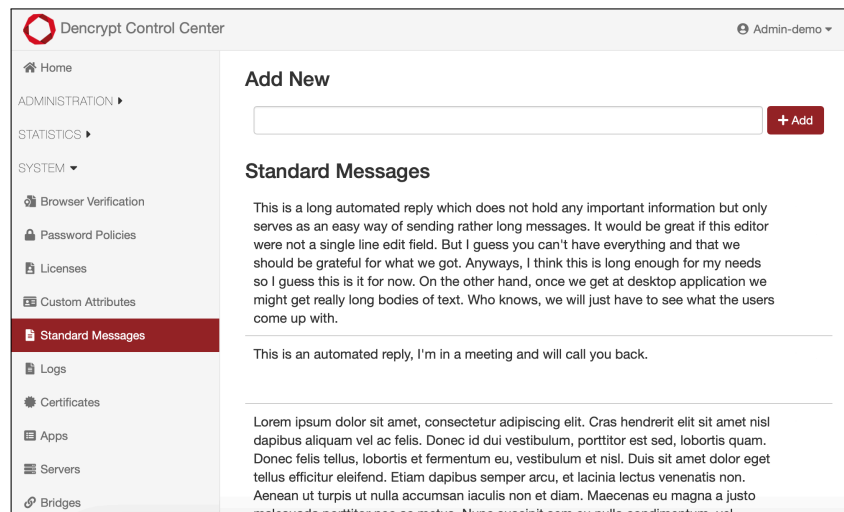


Figure 68: Frontpage for standard messages.

7.19.1 Create standard message

Create standard message

Step 1: Enter a message text in the *Add new* field.

Step 2: Tap *Add*.

Parameters:

Add new Text for the new standard message.

Outputs:

- New standard message created.
-

7.19.2 Edit standard messages

Edit standard messages

Step 1: Select the standard message.

Step 2: Select the pencil icon to edit the message. Tap *Save*.

Step 3: Select the garbage bin to delete the message. Confirm the warning.

Step 4: Select up/down arrows to change the order of messages.

Parameters:

Text Text for the standard message.

Outputs:

- Updated or deleted message.
 - Updated order of messages.
-

7.20 Custom Attributes

Custom Attributes are end-user-associated attributes that may be configured for the system.

Access frontpage for Custom Attributes

Step 1: Open *System* → *Custom Attributes*.

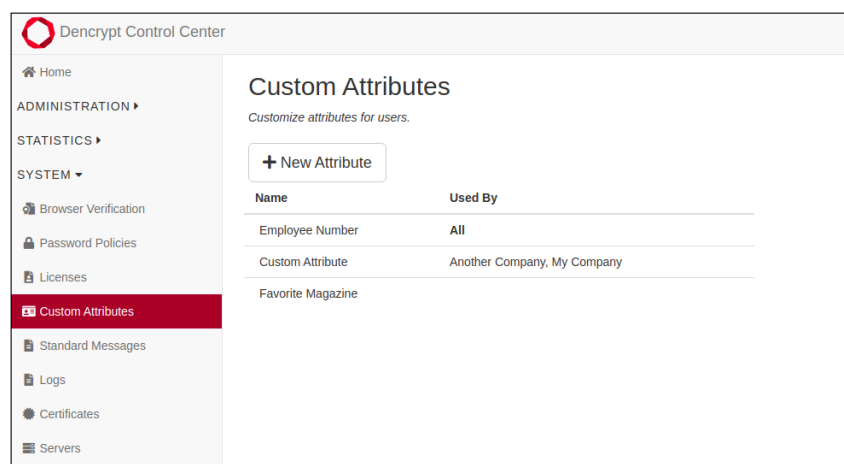


Figure 69: Frontpage for custom attributes.

7.20.1 Create Custom Attributes

Create a new custom attribute

Step 1: Click on *New Attribute*.

Step 2: Enter the name of the attribute.

Step 3: Select whether it is used for all companies or only selected companies.

Step 4: (Optional) Select the companies that use the attribute.

Parameters:

Name of the new attribute.

Companies to use the attribute.

Outputs:

- New custom attribute.

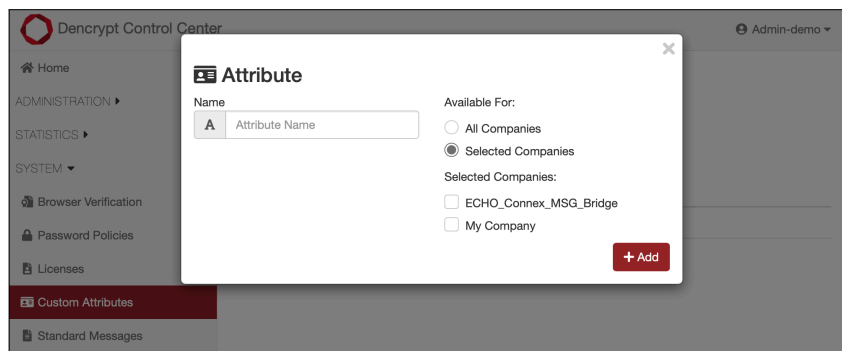


Figure 70: Create a custom attribute.

7.20.2 Edit attribute

Edit attribute

Step 1: Click the attribute in the list to edit.

Step 2: Write the new name of the attribute. Tap *Save*.

Step 3: Change which companies the attribute is used by.

Step 4: Tap *Save*.

Parameters:

Text of new attribute name.

Companies the attribute is used by.

Outputs:

- Attribute is now updated.

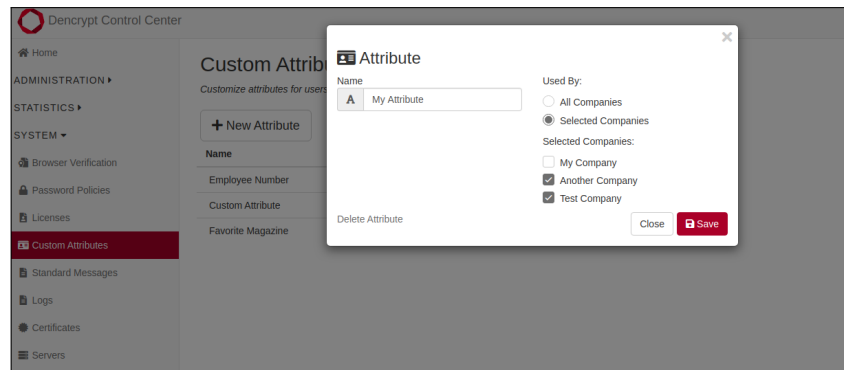


Figure 71: Edit a custom attribute.

7.20.3 Set User Attribute

Set the value of a custom attribute for a user

Step 1: Open *Administration* → *Users*.

Step 2: Click the user you wish to edit. Bulk edit may be used to set custom attributes for multiple users.

Step 3: Click *Details* and write the value of the custom attribute and press *Save*

Parameters:

Value of the custom attribute.

Outputs:

- Value of the custom attribute for the user is now set.

7.20.4 Order By Custom Attribute

Order users by their custom attribute

Step 1: Open *Administration* → *Users*.

Step 2: Click the icon on the right side of the user table.

Step 3: Tick the custom attribute on and press *Save*.

Parameters:

None.

Outputs:

- A custom with the custom attribute is now shown in the list.

7.21 Audit logs

Audit logs are collected for all events performed in the Dencrypt Control Center and for all successful and unsuccessful connections to the server components. The following events are logged:

- Login (both successful and unsuccessful attempts).
- Changes to system configurations.
- All changes to users, groups, departments, companies and administrators.
- Invitations, revocations and deletion of users.
- SSH connections for all server components
- TLS connections for all server components.
- Error messages.

Access audit logs

Step 1: Open *System* → *Logs*.

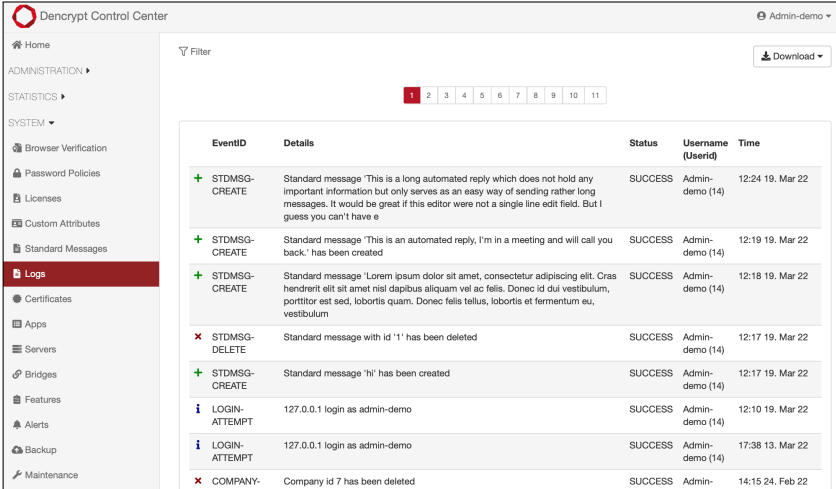
Step 2: Select *Filter* to filter logs according to *EventID* and time period.

Step 3: Select *Download* to download log files (.csv) per server component.

Outputs:

- Display list of DCC events including *EventID*, *Description*, *Status*, *Username (admin)*, *timestamp*.
- Downloaded log file per server component.

A complete list of DCC events with details is available in [Audit logs definitions B],



EventID	Details	Status	Username (Userid)	Time
+ STDMSG-CREATE	Standard message 'This is a long automated reply which does not hold any important information but only serves as an easy way of sending rather long messages. It would be great if this editor were not a single line edit field. But I guess you can't have e	SUCCESS	Admin-demo (14)	12:24 19. Mar 22
+ STDMSG-CREATE	Standard message 'This is an automated reply, I'm in a meeting and will call you back.' has been created	SUCCESS	Admin-demo (14)	12:19 19. Mar 22
+ STDMSG-CREATE	Standard message 'Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras hendrerit elit sit amet nisl dapibus aliquam vel ac felis. Donec id dui vestibulum, porttitor est sed, lobortis quam. Donec felis tellus, lobortis et fermentum eu, vestibulum	SUCCESS	Admin-demo (14)	12:18 19. Mar 22
× STDMSG-DELETE	Standard message with id '1' has been deleted	SUCCESS	Admin-demo (14)	12:17 19. Mar 22
+ STDMSG-CREATE	Standard message 'hi' has been created	SUCCESS	Admin-demo (14)	12:17 19. Mar 22
i LOGIN-ATTEMPT	127.0.0.1 login as admin-demo	SUCCESS	Admin-demo (14)	12:10 19. Mar 22
i LOGIN-ATTEMPT	127.0.0.1 login as admin-demo	SUCCESS	Admin-demo (14)	17:38 13. Mar 22
× COMPANY-REMOVE	Company id 7 has been deleted	SUCCESS	Admin-demo (14)	14:15 24. Feb 22

Figure 72: Audit logs.

7.22 Password policy

Password policies are defined by administrators with *Service access* role.

Access password policy

Step 1: Open *System* → *Password Policies*

Step 2: Applies policies.

Step 3: Tap *save*

Parameters:

Length	Minimum amount of characters required.
Max Age (Days)	The duration until a change password is enforced. Set to "0" to disable.
Min Age (Hours)	The minimum frequency for changing the password.
Password history	Define the number of unique passwords before reuse is allowed.
Login Attempts	Maximum attempts before the account is locked.
Req. Capital Letter	Require at least one capital letter in the password.
Req. Special Char.	Require at least one special character in the password.
Req. Numeric Char.	Require at least one numeric character in the password.

Outputs:

- Updated password policy.

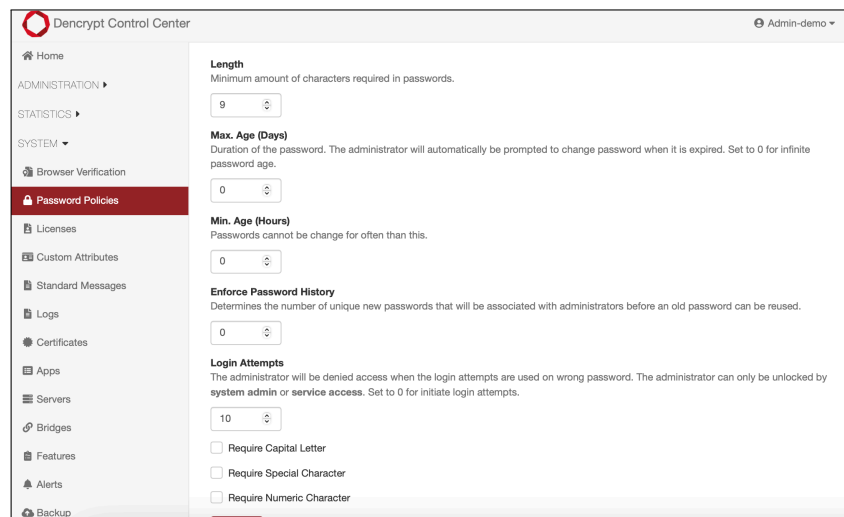


Figure 73: Define password policy

7.23 Server status

Monitor status for each server component:

- Status and system load: CPU load, memory usage and disk space used.
- Certificate status and expiry date.
- Configuration.
- Version number for applied libraries.
- System load history and server alerts.
- Renaming server component.

Display system status.

Step 1: Open *System* → *Servers*.

Parameters:

Status	OK, Warning or Error.
System load	CPU load, memory usage and disk space used.
Certificate	Status and expiry date.
History	System load history and server alerts.
Version	Version number for the server component and applied SW libraries.
Rename	Naming the server component.

Outputs:

- Dashboard showing the current status and load of the Dencrypt Communication Servers.

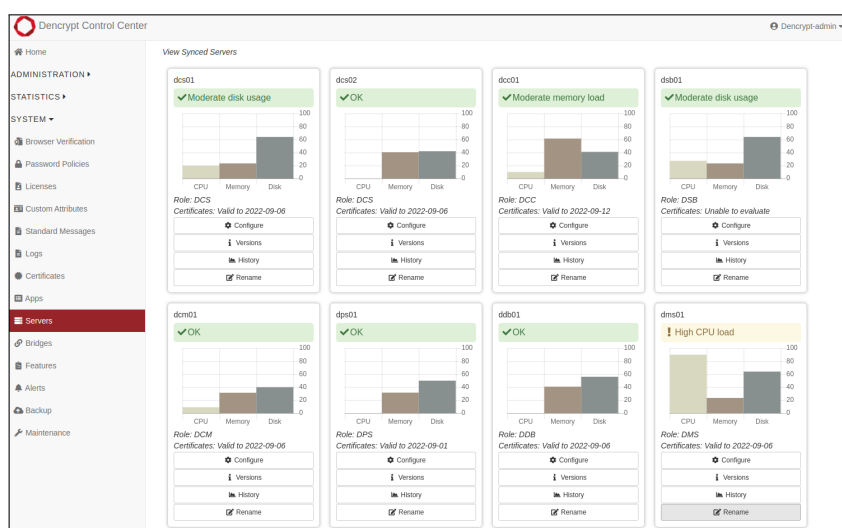


Figure 74: Dashboard for server status

7.24 Manage bridge connections

When phonebook data changes, the data shared with the remote systems are automatically updated.

Manage remote connections

Step 1: Open *System* → *Bridges*.

Step 2: Tap *Sync data (Remote to local)* to manually pull data from the selected remote system.

Step 3: Tap *Sync data (Local to remote)* to manually push data from the selected remote system.

Step 4: Tap *Check connections* to refresh system statuses

Parameters:

Connection request missing	Remote system defined. Await generation of own connection request.
Pending	Await connection request from the remote system.
Active	Bridge connection established.

Outputs:

- Display *System ID, system name, DNS address, Port* of own system.
- Display *System ID, system name, DNS address, Port, state, last update* of the remote server systems.
- A new connection to the remote system is established.

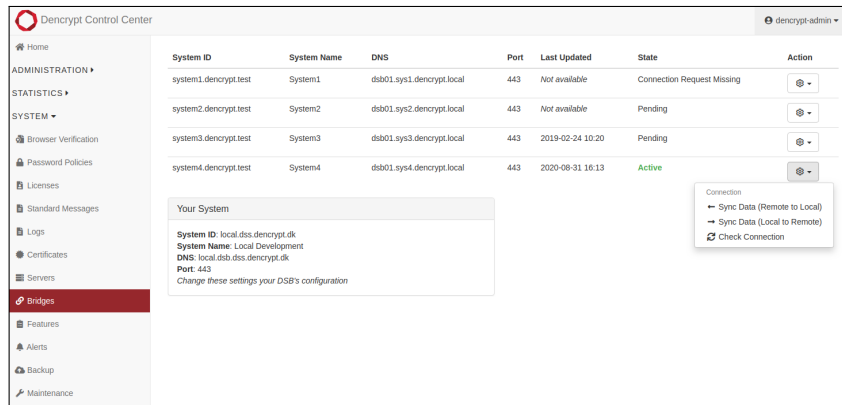


Figure 75: Manage remote connections.

7.25 Certificates

7.25.1 Servers

Display server certificates

- Step 1: Open *System* → *Certificates*.
- Step 2: Select *Servers* tap to display server certificates.
- Step 3: Select a server component to expand certificate details.
- Step 4: Select *Install certificates* to re-install certificates.

Outputs:

- An overview of the certificate status and expiry date.
- Detail per server component. Status and expiry of applied server certificates.

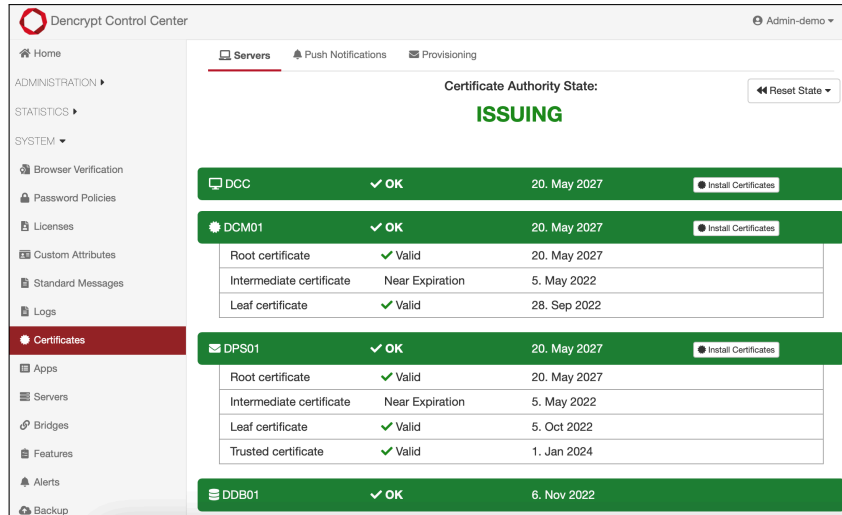


Figure 76: Server certificates.

7.2.5.2 Push Notifications certificates

Display push certificate details.

Step 1: Open *System* → *Certificates*.

Step 2: Select *Push Notifications* tap to display push certificates.

Parameters:

AppID: Identification of the application the certificate belongs to.

Cert Type: Production or Development.

Issuer: The issuer of the push certificate. Apple or Google.

Capabilities: Which capabilities the push certificate is configured for.

Expires: When the certificate expires.

Outputs:

- Details of installed certificates.

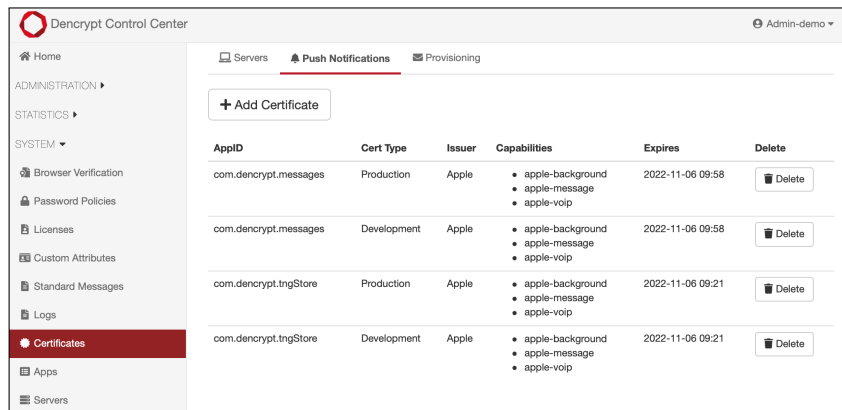


Figure 77: Push notification certificates.

Install push certificate.

-
- Step 1: Open *System* → *Certificates*.
- Step 2: Select *Push Notifications* tap to display push certificates.
- Step 3: Click *Add Certificate*
- Step 4: Select Application in the dropdown.
- Step 5: Select *Cert Type* as Production or Development.
- Step 6: Select one or more capabilities of the certificate.
- Step 7: Select whether the certificate is a file or text and the content of the certificate.
- Step 8: Tap *+Add*.
- Step 9: To delete certificates: Tap *Delete*
-

Parameters:

Application: A list of all applications installed on the system.

Cert Type: Production or Development.

Capability: Which capability the push certificate is configured for.

File

Certificate file provided by Dencrypt

Outputs:

- New certificate installed or removed.
-

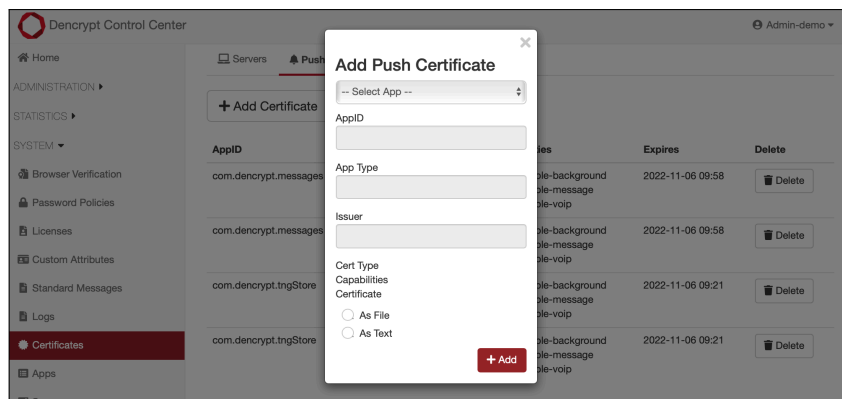


Figure 78: Create new push notification certificate.

7.25.3 Provisioning Certificates

View existing provisioning certificates

-
- Step 1: Open *System* → *Certificates*.
- Step 2: Select *Provisioning* tap to display push certificates.
-

Parameters:

Status: Whether the certificate is currently active or revoked.

Tag: Free text associated with the certificate

Issued: Timestamp for when the certificate was issued.

Expires: Timestamp for when the certificate expires.

Action Download: Retrieve a copy of the key and certificate that will be downloaded to the local computer.

Action Re-tag: Change the tag of an existing certificate.

Action Revoke: Revoke a certificate, rendering it invalid for provisioning.

Outputs:

- Details of provisioning certificates.

Generate new provisioning certificate

Step 1: Open *System* → *Certificates*.

Step 2: Select *Provisioning* tap to display provisioning certificates.

Step 3: Fill out form in *Generate New* section and press *Generate*.

Parameters:

Tag: Free text associated with the certificate

Duration: The number of days until the certificate expires.

Outputs:

- New certificate is generated
-

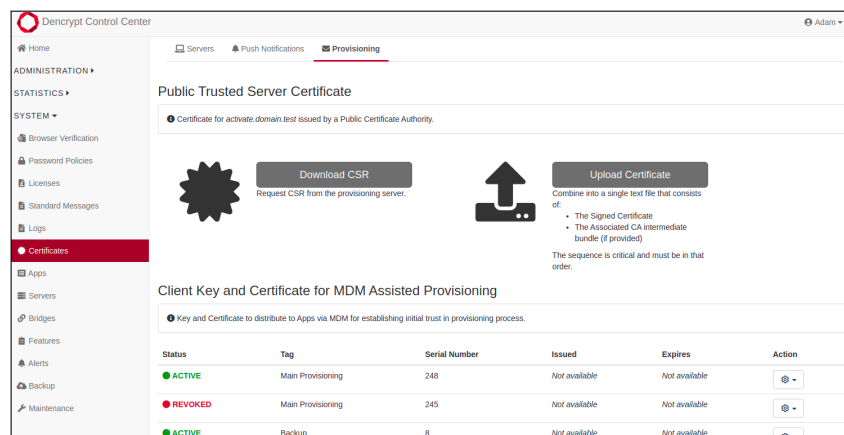


Figure 79: Provisioning Certificates.

7.26 Features

Features specify additional configurations of the end-user devices, such as enforcing biometric login or disabling phonebook caching. Only administrators with *Service access* role can update features.

Display feature settings

Step 1: Open *System* → *Features*.

Outputs:

- Display the active features and global settings for the end-user devices

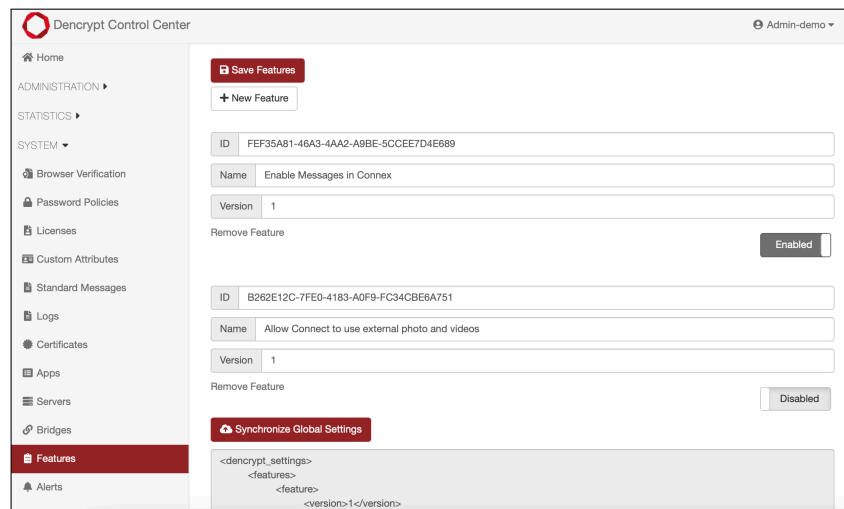


Figure 80: Display active features.

7.27 Manage alerts

Alerts are used to send email notifications on system errors and events and for sending monthly system reports.

Manage alerts

Step 1: Open *System* → *Alerts*.

Step 2: Configure SMTP email account: Enter *Hostname*, *Protocol*, *port*, *username*, *password* and *sender*. Tap *Save*

Step 3: Configure notifications:

- Enter the email address of the recipients.
- Check which event to trigger a notification.
- Tap *Save*
- Tap *Send notification* to send notification now.

Step 4: Configure system reports:

- Enter the email address of the recipients.
- Tap *Save*
- Tap *Send report* to send a status report now.

Parameters:

<i>Host</i>	Hostname for email server
<i>Protocol</i>	Applied protocol: SMTP, SSL, TLS
<i>Port</i>	SMTP port number
<i>Username/password</i>	Credential for accessing email server
<i>Send from</i>	Senders email address.
<i>Email</i>	Recipients email address

Outputs:

- Updated email account.
- Configuration and Recipient of notifications.
- Recipient for monthly system reports.

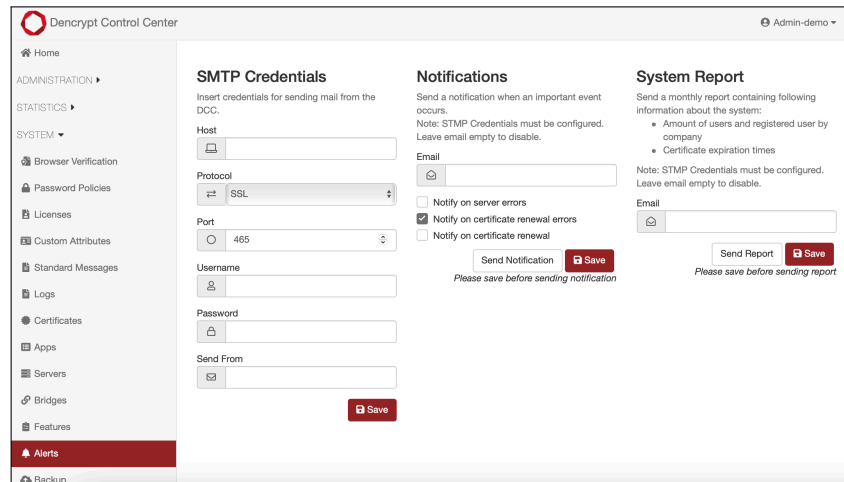


Figure 81: Manage alerts.

7.28 Manage backup

Encrypted backup of system data is configured at the time of system installation, where also the PGP key pair is generated. An administrator with *System admin* role can reconfigure the backup and run an immediate backup.

To run a backup

- Step 1: Open *System* → *Backup*.
- Step 2: Select destination by checking *Remote* or *local*.
- Step 3: Tap *Backup now*

Parameters:

- Remote* Backup destination is a remote server.
Local Download a backup to the local server

Outputs:

- Encrypted backup stored on a remote and/or a local machine.

Configure backup

- Step 1: Open *System* → *Backup*.
- Step 2: Check *Enabled* under *Remote backup*.
- Step 3: To change destination: Enter address, credentials, file path and filename.
- Step 4: To change schedule: Enter time and date under *schedule*.
- Step 5: Tap *Save*

Parameters:

Destination	SCP or SFTP
Connection	Server address and port
Password	Password to remote server
Remote folder	Destination path
Filename	Destination file (*.zip). Check to append the date to file-name

Outputs:

- Updated destination for remote backups.
- Updated backup schedule.

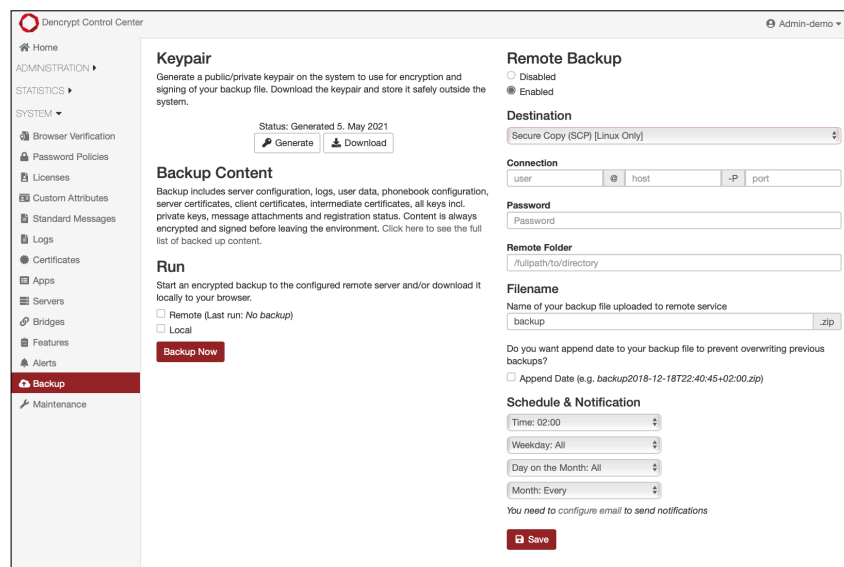


Figure 82: Manage backup

7.29 Display operational mode

Display the operational mode

Step 1: Open *System* → *Maintenance*.

Outputs:

- List of operational modes per server component.

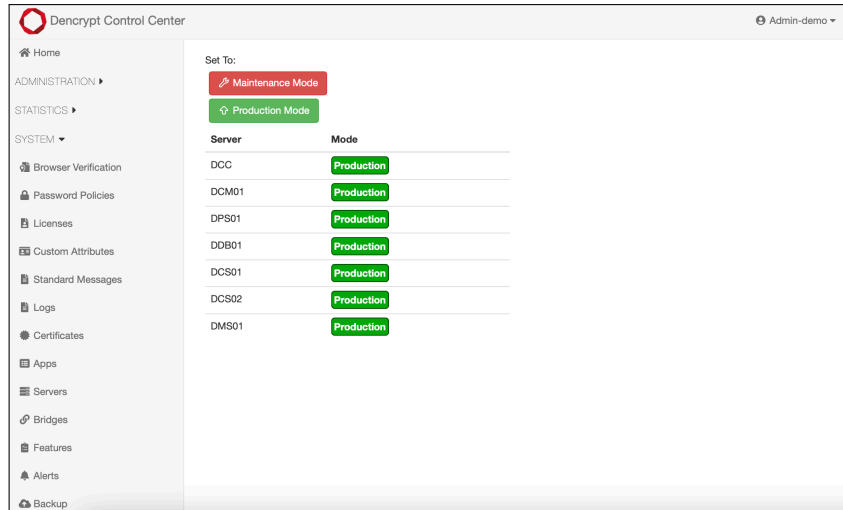


Figure 83: System operational mode

8 DSS REST API

The DSS REST API provides an alternative interface that allows 3rd parties to manage organizations and users in the Dencrypt Server System. Typical examples of use are:

- Create company, department, groups and users
- Invite users
- Revoke and/or delete users

The API is protected by an API key, which is associated with a DCC Administrator, but as it is not secured by TLS client authentication, access should be restricted and only exposed to trusted users.

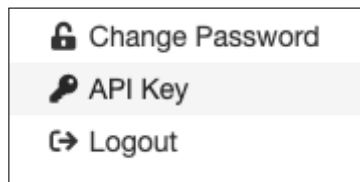
8.1 API endpoints

A full list of all possible calls can be seen by accessing https://DCC_SERVER_IP/api/admin/v1-0/docs in a browser. This will reveal a complete spec of the API. This spec follows the API version and will therefore always correspond to the actual API.

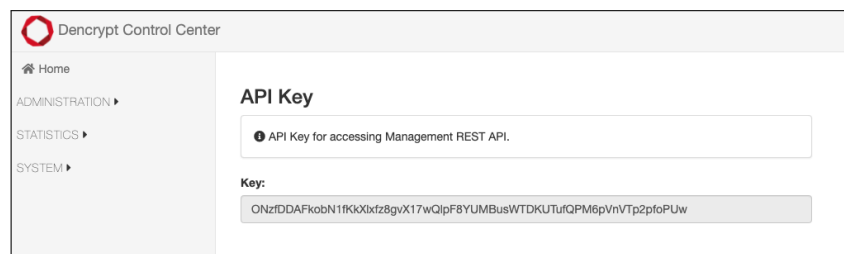
8.2 Authentication

To make a call to the API, a user must be authenticated. This is done through the authentication key obtained in DCC. The authentication key is then passed along with the API call. See the section [Examples 8.3], for examples of where and how to include the authentication key.

To obtain the key, go to the top right corner of the DCC and select "API key":



This will show the following view where the key can be copied from.



8.3 Examples

Examples of use (using curl):

- Download the "Browser Verification" certificate from the DCC and use it as a CA certificate file in the curl requests.
- For the server IP, use the IP address or DNS entry of the DCC.
- The authentication key is included as "apiKey" followed by the actual key. The content is included as JSON.

Create a company called "Corporate Inc"

```
curl --cacert [CA certificate file] --location --request POST 'https://[server IP]/  
  ↪ api/admin/v1-0/company' \  
--header 'Authentication: apiKey  
  ↪ gPhV1kkRa9nLvkHSAP7hstFzZdrKvYIHPYDyRIHcvjBpPP3SSWK311kD5JAZpolk' \  
--header 'Content-Type: application/json' \  
--data-raw '{  
  "companyName" : "Corporate Inc"  
}'
```

This will return a status code and a data field including the assigned companyId

```
{"status": "OK", "data": "175"}
```

Create a department called "IT Department"

```
curl --cacert [CA certificate file] --location --request POST 'https://[server IP]/  
  ↪ api/admin/v1-0/department' \  
--header 'Authentication: apiKey  
  ↪ gPhV1kkRa9nLvkHSAP7hstFzZdrKvYIHPYDyRIHcvjBpPP3SSWK311kD5JAZpolk' \  
--header 'Content-Type: application/json' \  
--data-raw '{  
  "departmentName" : "IT Department",  
  "companyId" : "175"  
}'
```

This will return a status code and a data field including the assigned departmentId

```
{"status": "OK", "data": "148"}
```

Create a user called "John Doe"

```
curl --cacert [CA certificate file] --location --request POST 'https://[server IP]/  
  ↪ api/admin/v1-0/user' \  
--header 'Authentication: apiKey  
  ↪ gPhV1kkRa9nLvkHSAP7hstFzZdrKvYIHPYDyRIHcvjBpPP3SSWK311kD5JAZpolk' \  
--header 'Content-Type: application/json' \  
--data-raw '{  
  "UserSchema": {  
    "firstName" : "John",  
    "lastName" : "Doe",  
    "email" : "johndoe@corporateinc.com",  
    "phoneNumber" : "12345678",  
    "companyId" : "175",  
    "departmentId" : "148",  
    "title" : "Manager"  
  }  
}'
```

This will return a status code and a data field including the assigned userId

```
{"status": "OK", "data": "j.dt1a2b3c4"}
```


A Advanced management functions

The functionalities described in this section are intended for maintenance only and are only available for the *Service Access* role. These functionalities shall only be used by Dencrypt technical personnel or IT professionals, who have received training in installing and configuring a Dencrypt Server System.

A.1 Change of operational mode

The operational mode of the Dencrypt Server System can be in:

1. **Production mode** - normal operational mode where end-user devices can connect to the server system to establish a secure voice call or secure message exchange.
2. **Maintenance mode** - used during service windows for upgrade or reconfiguration of the server system. End-users are prevented access to the server system.

Change of operational mode

Step 1: Open *System* → *Maintenance*

Step 2: Tap *Maintenance mode* and confirm the warning to enter the maintenance mode.

Step 3: Tap *Production mode* and confirm the warning to enter the operational mode.

Outputs:

- Changed operational mode of the Dencrypt Server System.

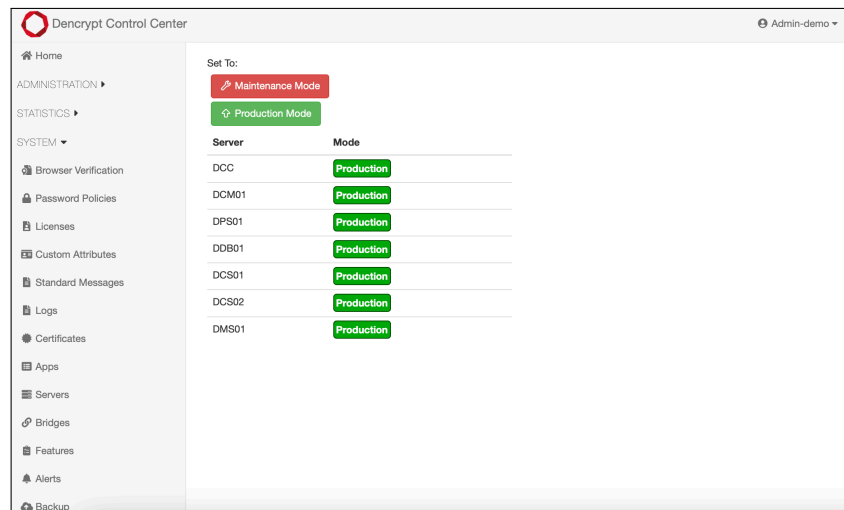


Figure 84: Toggle operational mode.

A.1.1 Configuration Change

Configuration Change

Step 1: Fill in the fields.

Step 2: Tap *Save*.

Outputs:

- DCM server reconfigured.

Parameters:

Common Fields

<code>rabbit_mq/server_ip</code>	IP address of the RabbitMQ server. <i>Not edible.</i>
<code>common/name</code>	Internal name of the server.
<code>common/hostname</code>	The hostname part of the fully qualified domain name (FQDN). <i>Not edible.</i>
<code>common/hostname</code>	The hostname part of the fully qualified domain name (FQDN). <i>Not edible.</i>
<code>common/system_domain</code>	DNS of the system domain.
<code>common/external_ip</code>	External IP for servers with the external interface.
<code>common/dns</code>	DNS entry.
<code>common/server_type</code>	Internal server abbreviation of the server type. <i>Not edible.</i>
<code>common/network_type</code>	Whether network type is configured as NAT or DirectIP.
<code>HAProxy/./name</code>	Internal technical name of the interface.
<code>HAProxy/./frontend</code>	Address to receive traffic from.
<code>HAProxy/./backend</code>	Address to send traffic to.
<code>HAProxy/./verify</code>	Whether to verify client certificate in TLS
<code>HAProxy/./curve</code>	Curve to accept
<code>HAProxy/./server</code>	Type of server to be specified in the HAProxy configuration file
<code>HAProxy/./crl</code>	Whether to reject connections in the certificate revoke list
<code>HAProxy/./certificate</code>	Which certificate on the server to use
<code>certificates/common_name</code>	Common name used in the HTTPS certificates.

A.2 Dencrypt Control Center: Configuration

Parameters:

DCC Configuration

<code>HAProxy/WebSSL/..</code>	Web interface for administrators.
--------------------------------	-----------------------------------

A.3 Dencrypt Certificate Manager: Configuration

Parameters:

DCM Configuration

<code>provisioning_certificate_expiry_hours</code>	Hours certificate is valid after issuance.
<code>ddb_connection/ip</code>	Hours certificate is valid after issuance.
<code>ddb_connection/port</code>	The port to connect to the DDB.
<code>ddb_connection/webapi_port</code>	Port for WebAPI.
<code>HAProxy/ExternalHTTPS/..</code>	Client interface for issuing and renewing certain client certificates.
<code>HAProxy/InternalHTTPS/..</code>	Internal server interface for web API requests.

A.4 Dencrypt Provisioning Server: Configuration

Parameters:

DPS Configuration

<i>ddb_internal_ip</i>	Internal IP of the DDB.
<i>dcm_internal_ip</i>	Internal IP of the DCM.
<i>invitation_expiry_time</i>	Amount of hours until the invitation is expired.
<i>invite_version</i>	Internal version of invitation. <i>Not edible</i> .
<i>permanent_invited_userids</i>	Space separated list of user IDs that can reuse invites AND never expires.
<i>reusable_invited_userids</i>	Space separated list of user IDs that can reuse invites.
<i>enable_legacy_provisioning</i>	Enable Dencrypt Talk provisioning.
<i>https_invite/enabled</i>	Whether to use unified HTTPS links for provisioning.
<i>mail_conf/mail_enabled</i>	Whether you should allow provisioning through email.
<i>mail_conf/mail_server</i>	Address of the mail server to use for email provisioning.
<i>mail_conf/mail_port</i>	Port of the mail server to use for email provisioning.
<i>mail_conf/mail_protocol</i>	Protocol of the mail server to use for email provisioning.
<i>mail_conf/username</i>	Username of the mail server to use for email provisioning.
<i>mail_conf/password</i>	Password of the mail server to use for email provisioning.
<i>mail_conf/mail_send_from</i>	Which email invites are seen as being sent from. If empty, it uses the username specified above.
<i>mail_conf/mail_voipgen1_subject</i>	Text of the email subject for VoipGen1.
<i>mail_conf/mail_voipgen1_name</i>	Name of the VoipGen1 application as presented in the email.
<i>mail_conf/mail_messagegen1_subject</i>	Text of the email subject for MessageGen1.
<i>mail_conf/mail_messagegen1_name</i>	Name of the MessageGen1 application as presented in the email.
<i>mail_conf/mail_multicomgen1_subject</i>	Text of the email subject for MultiComGen1.
<i>mail_conf/mail_multicomgen1_name</i>	Name of the MultiComGen1 application as presented in the email.
<i>mail_conf/logo</i>	Name of the logo file on local server <code>/usr/local/dencrypt/dcs/emails/*</code> .
<i>mail_conf/logo_alt_text</i>	Alternative text if the logo is not loaded or prior to showing the logo.
<i>mail_conf/customer</i>	Name of the customer presented in the invitation.
<i>mail_conf/supportEmail</i>	Support email presented in the invitation.
<i>mail_conf/supportPhone</i>	Support phone number presented in the invitation.
<i>mail_conf/retry_delay</i>	Number of seconds to wait before retrying to send the email.
<i>sms_conf/sms_enabled</i>	Whether you should allow provisioning through SMS.
<i>sms_conf/method</i>	GET or POST request method to SMS provider.
<i>sms_conf/url</i>	Full URL to SMS service. Use receiver, message and sender as variables, encapsulated with curly brackets.
<i>sms_conf/body</i>	Raw body of POST request. Ignored for GET requests. Use receiver, message and sender as variables, encapsulated with curly brackets.
<i>sms_conf/headers</i>	List of HTTP headers, separated by semicolon. Use receiver, message and sender as variables, encapsulated with curly brackets.
<i>sms_conf/talk_text</i>	Prepended text in the SMS for VoipGen1.
<i>sms_conf/messages_text</i>	Prepended text in the SMS for MessageGen1.
<i>sms_conf/dencrypt_text</i>	Prepended text in the SMS for MultiComGen1.
<i>sms_conf/sender</i>	Subject of the SMS sender.
<i>certificates/provisioning</i>	Common name used for provisioning.
<i>HAProxy/ExternalHTTPS/..</i>	Client interface for provisioning when accepting invitations.
<i>HAProxy/InternalHTTPS/..</i>	Internal server interface for web API requests.

A.5 Dencrypt Database: Configuration

Parameters:

DDB Configuration

<i>db_conf/db</i>	Database name to connect to.
<i>db_conf/user</i>	Database username to connect with.
<i>db_conf/password</i>	Database password.
<i>db_conf/ip</i>	Database address.
<i>db_conf/port</i>	Database port.
<i>phonebook/show_unregistered_users</i>	Whether to show unregistered users in the phonebook.
<i>phonebook/sip_domain</i>	The sip domain for VoipGen1.
<i>phonebook/xmpp_domain</i>	The xmpp domain for MessageGen1.
<i>HAProxy/InternalHTTPS/..</i>	Internal server interface for web API requests.

A.6 Dencrypt Communication Server: Configuration

Parameters:

DCS Configuration

<i>srvrec_name</i>	DNS of the subdomain for server records.
<i>db_password</i>	Password for database connection.
<i>ddb_ip</i>	Internal IP of the DDB.
<i>authorization</i>	Whether to authorize user ID and password for WebAPI.
<i>allow_meta_data_in_push</i>	Allow metadata such as name, SIP address etc. in push notifications.
<i>push_encryption</i>	Encrypt content of push notifications.
<i>call_push_ttl</i>	Time to live in seconds for call push notifications.
<i>db_conf/db</i>	Database name to connect to.
<i>db_conf/user</i>	Database user to connect with.
<i>db_conf/password</i>	Database password to connect with. <i>Not edible</i> .
<i>db_conf/ip</i>	Database IP to connect to.
<i>db_conf/port</i>	Database port to connect to.
<i>ddb_connection/ip</i>	The IP of the DDB.
<i>ddb_connection/port</i>	The port to connect to the DDB.
<i>flexisip/proxy_enabled</i>	Whether to enable Flexisip Proxy server.
<i>flexisip/conference_enabled</i>	Whether to enable Flexisip Conference server.
<i>flexisip/presence_enabled</i>	Whether to enable Flexisip Presence server.
<i>flexisip/log_level</i>	Verbosity of logs to output.
<i>flexisip/conference_factory</i>	Uri where the client must ask to create a conference. Example: sip:conference-factory@dcs.charlie.dss.dencrypt.local.
<i>flexisip/conference_outbound_proxy</i>	Example: sip:10.10.20.184:5070;transport=tcp.
<i>flexisip/sip_port</i>	SIP port to listen on (DEPRECATED - use transports instead).
<i>flexisip/transports</i>	Transports parameter of Flexisip defining interfaces to listen on. Example: sips:dcs01.mysystem.example.com:5061;maddr=192.168.5.10.
<i>flexisip/auth_domains</i>	Space separated.
<i>flexisip/nodes</i>	Space separated.
<i>flexisip/trusted_hosts</i>	Space separated.
<i>flexisip/aliases</i>	Space separated.
<i>flexisip/reg_domains</i>	Space separated.
<i>flexisip/webapi</i>	The address for the WebAPI phonebook and settings download.
<i>flexisip/redis_server</i>	Redis address.
<i>flexisip/redis_port</i>	Redis port.
<i>flexisip/enable_call_logs</i>	Whether to enable call logs.
<i>flexisip/udp_min_port</i>	Lower limit for UDP ports used for media relay.
<i>flexisip/udp_max_port</i>	Upper limit for UDP ports used for media relay.
<i>flexisip/force_public_ip_for_sdp_masquerading</i>	Force public IP in SDP (needed when Flexisip is behind NAT and HAProxy).
<i>flexisip/devices_per_user</i>	Number of devices allowed per user.
<i>lime/curve_id</i>	Curve to use, shall be either CurveId::CURVE25519 or CurveId::CURVE448.
<i>lime/persistent_connections</i>	Whether to persist connection.
<i>lime/lime_db_host</i>	Lime database host.
<i>lime/lime_db_name</i>	Lime specific database name to connect with.
<i>lime/log_level</i>	Log level of Lime. Disabled is recommended.
<i>lime/db_logs_enabled</i>	Whether database logs are enabled.
<i>lime/auth_realm</i>	Typically same as system domain.
<i>lime/auth_nonce_key</i>	Random string(12 characters minimum length) specific to each server and is private. Leave empty to autogenerate a 20-character long string.
<i>lime/min_nonce_validity_period</i>	The authentication is aimed to provide a one-time usage nonce, it is not strictly enforced by storing valid once, instead we use a short living period, the maximum validity period will be twice the minimum one, value is in seconds.
<i>certificates/service_records</i>	Common name used for SIPS certificates.
<i>public_interfaces/webapi_port</i>	Port to public WebAPI.
<i>public_interfaces/sip_port</i>	Port to public SIP.

A.7 Dencrypt System Bridge: Configuration

Parameters:

DSB Configuration

<i>internal_port</i>	Internal port used for bridge interface.
<i>external_port</i>	External port used between bridges.
<i>haproxy_bridge_config</i>	HAProxy config file for bridge interfaces.

A.7.1 Create a remote system connection

To federate two server systems, the system administrator will create a remote system and establish a trusted connection.

Create a new remote system

Step 1: Open *System* → *Bridges*. to display a list of remote systems.

Step 2: Enter *Remote System ID* and tap *New* to create a new remote system.

Step 3: Status of the created system is: *Connection Request Missing*.

Parameters:

System ID System identifier

Outputs:

- New remote system created.

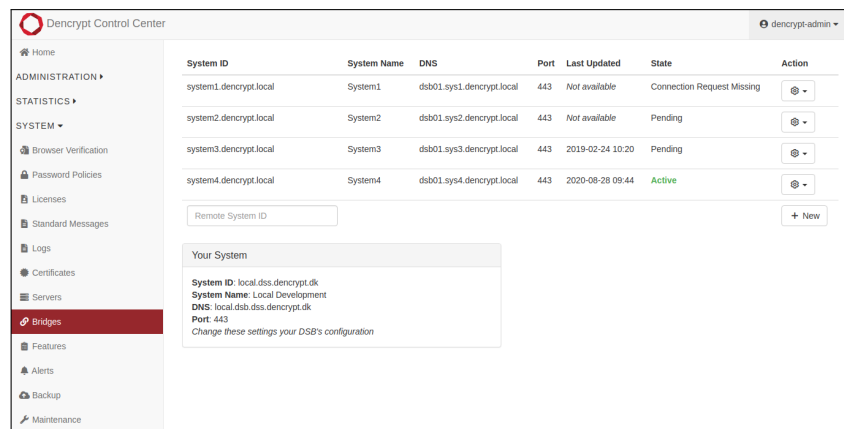


Figure 85: Remote systems.

Establish a trusted connection.

- Step 1: Open *System* → *Bridges*.
- Step 2: Select the remote system and tap *Actions*.
- Step 3: Tap *Export Connection Request* and download the certificate-file: `connection-request-<systemid>-<date>.json`.
- Step 4: The certificate file is delivered securely to the remote administrator using encrypted email or encrypted drives. **The certificate file may not be disclosed to 3rd parties.**
- Step 5: To install a received certificate from the remote system: Tap *Import connection request* and install the file received from the remote administrator.
- Step 6: Await the remote system to become available. System status is *Pending* until certificates have been installed in the remote system. Tap *Check connection* to refresh statuses.
- Step 7: The federation is established and the status is *Active*.

Parameters:

<i>Connection request missing</i>	Remote system defined. Await generation of own connection request.
<i>Pending</i>	Await connection request from the remote system.
<i>Active</i>	Bridge connection established.

Outputs:

- Remote connection established.

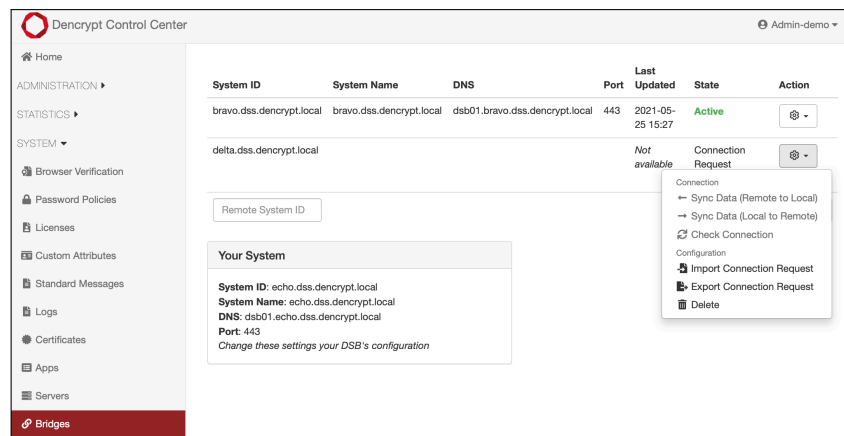


Figure 86: Establish a remote connection.

A.7.2 Delete a remote system connection.

The federated connection to a remote system can be deleted and certificates revoked by an administrator with *Service access* privileges.

Revoke a system connection

Step 1: Open *System* → *Bridges*.

Step 2: Tap *Delete* to remove a system connection and revoke certificates. See figure 86.

Step 3: Confirm the warning.

Outputs:

- Remote system deleted and certificates revoked.

The connection to the remote system can only be restored by establishing a new connection [Establish a server federation 6.1].

A.8 Features configuration

Dencrypt Connex features can be defined and modified server-side. Feature settings are included in the *Global settings*, which are provided to the Dencrypt Connex next time it connects to the server system.

This functionality is only available for the *Service Access* role.

Create and modify features

Step 1: Open *System* → *Features*.

Step 2: To create a new feature: Tap + *New Feature*.

Step 3: Fill in feature ID, feature name and version.

Step 4: Toggle *Enabled/disabled* to activate de-activate the feature.

Step 5: To delete a feature: Tap *Remove feature* and confirm the warning.

Step 6: To refresh global settings: Tap *Synchronize Global Settings*.

Parameters:

- ID** Unique feature identifier.
Name Descriptive name of the feature.
Version Feature version number.

Outputs:

- Feature created, modified, removed, enabled or disabled.

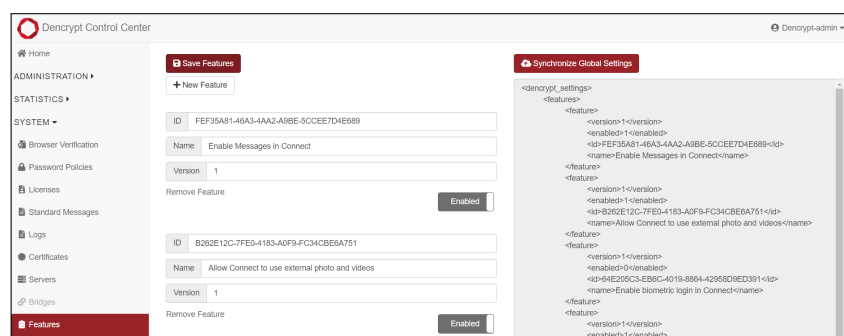


Figure 87: Feature configuration.

A.9 SSH access

SSH access to the virtual machine environment of a server component is required to perform a software update. Access is only possible from within the Customer's secure environment. To access a terminal window (shell prompt) to the virtual machine:

Syntax: `ssh <username><component>.<domainname>`,

where *username*, *component* and *domain name* are defined during system installation. Dencrypt does not generate passwords unless requested by the customer who owns the system, in which case, the password is generated following the password policy [Password Policy 2.11]. Ordinarily, the customer provides passwords according to their company policies.

B Audit logs definitions

Table 2: Audit log definitions

Event ID	Description	Type	Details
ADMIN-ADD	Admin: Add account	create	Administrator <username> created.
ADMIN-LOCK	Admin: Lock account	delete	Admin with id <adminid> now is now locked.
ADMIN-PWRESET	Admin: Reset password	update	Admin with id <adminid> has had reset password
ADMIN-REMOVE	Admin: Delete account	delete	Administrator id <adminid> deleted.
ADMIN-UNLOCK	Admin: Unlock account	create	Admin with id <adminid> now is now unlocked.
ADMIN-UPDATE	Admin: Configure account	update	Admin with id <adminid> has changed role to <newrole>
ADMIN-UPDATE	Admin: Configure account	update	Admin with id <adminid> now has permission to company id <companyid>
ADMIN-UPDATE	Admin: Configure account	update	Admin with id <adminid> has no longer permission to company id <companyid>
BACK-AUTO	Backup: Configuration updated	update	Backup configuration updated.
BACK-DOWNLOAD	Backup: Manual backup	info	Backup downloaded.
BACK-GETKEY	Backup: Received keys	info	Keypair retrieved.
BACK-KEYGEN	Backup: Keypair generated	create	Keypair generated
BACK-REMOTE	Backup: Remote backup	info	Remote backup performed
BRIDGE-CREATE	Bridge: Add connection	create	Bridge connection for system <systemid> created.
BRIDGE-DELETE	Bridge: Delete connection	delete	Bridge connection for system <systemid> has been deleted.
BRIDGE-IMPORT	Bridge: Connection request	create	Bridge connection request imported for system <systemid>
CERT-CSR	Server: CSR	update	Initialized CSR request for DCM <serverid>
CERT-CSR	Server: CSR	update	CSR requested from DPS
CERT-IM	Server: Interm. certificate install	update	Install intermediate certificate for DCM <serverid>
CERT-RESET	Server: Certificate reset	update	State RESET to <state>.
CERT-ROOT	Server: Root certificate install	update	Installed root for DCM <serverid>
CERT-ROOTCRL	Server: CRL install	update	Upload root CRL for DCM <serverid>
CERT-TRUST-INSTALL	Server: Install public CA certificated	update	Certificate installed for DPS
COMPANY-ADD	Company: Add	create	Company <name> created.
COMPANY-REMOVE	Company: Delete	delete	Company id <companyid> has been deleted.
COMPANY-REMOVEGROUP	Company: Share group	delete	Group id <groupid> is no longer connected to company id <company id>
COMPANY-TOGROUP	Company: Unshare group	create	Group id <groupid> is now connected to company id <company id>
COMPANY-UPDATE	Company: Edit	update	Company <name> with id <companyid> has been updated.
DEP-ADD	Department: Add	create	Department <name> created.
DEP-DELETE	Department: Delete	delete	Department id <dep.id> has been deleted.
DEP-UPDATE	Department: Edit	update	Department id <dep.id> updated name to <newname>
EMERG-ADDCONTACT	Emergency list: Add user	create	User <id> has been added to emergency list <name>
EMERG-CREATE	Emergency list: Add	create	Emergency list <name> created.
EMERG-DELETE	Emergency list: Delete	delete	Emergency list <name> has been deleted.
EMERG-DELETE		delete	Emergency list <name> has been deleted.
EMERG-REMOVECONTACT	Emergency list: Remove user	delete	User <id> has been removed from emergency list <name>

Continued on next page

Table 2 – Continued from previous page

Event ID	Description	Type	Details
EMERG-SHARE	Emergency list: Share	create	Emergency list <name> has been made available to Company <companyid>
EMERG-UNSHARE	Emergency list: Unshare	delete	Emergency list <name> has been made unavailable to Company <companyid>
EMERG-UPDATE	Emergency list: Edit	update	Emergency list <name> has changed name to <newname>
GROUP-ADD	Group: Add	create	Group name: <groupid> created.
GROUP-REMOVE	Group: Delete	delete	Group id: <groupid> deleted.
GROUP-UPDATE	Group: Update	update	Group name: <groupid> changed name to <newname>
GROUP-UPDATE	Group: Update	update	Group id <groupid> link to group id <groupiod> is set to <link>
LOGIN-ATTEMPT	Admin login attempt	info	<ip> login as <admin.id>
MAINTENANCE-SET	Server: Toggle maintenance mode	update	Maintenance for server <id> set to on/off.
PUSH-ADD	Push certificate: Add	create	Push certificate added. Id: <cert id>
PUSH-REMOVE	Push certificate: Delete	delete	Push certificate removed Id: <cert id>
SERVER-ACTIVATE	Server: Toggle activation	update	Server: <id> activation status set to enabled/disabled.
SERVER-ADD	Server: Add	create	Server created at <IP>
SERVER-CONFIG	Server: Configuration update	update	Server: <id> configuration updated.
SERVER-REMOVE	Server: Remove	delete	Server: <id> has been deleted
SERVER-UPDATE	Server: Change IP and API-key	update	Server <id> changed IP to <IP> and API key.
SERVER-UPDATE	Server: Change API-key	update	Server <id> changed API Key
SERVER-UPDATE	Server: Change IP-address	update	Server <id> changed IP to <IP>.
STDMSG-CREATE	Std Messages: Add	create	Standard message <msgid> has been created.
STDMSG-DELETE	Std Messages: Delete	delete	Standard message with id <msgid> has been deleted.
STDMSG-ORDER	Std Messages: Move up	update	Standard message with id <msgid> has been moved up in order.
STDMSG-ORDER	Std Messages: Move down	update	Standard message with id <msgid> has been moved down in order.
STDMSG-UPDATE	Std Messages: Edit	update	Standard message with id <msgid> has been updated
SYS-FEATURE	System: Feature configuration	update	Feature settings updated
SYS-NOTIFICATION	Notifications: Update	update	Alert SMTP credentials updated.
SYS-NOTIFICATION	Notifications: Update	update	Alert notification updated
SYS-NOTIFICATION	Notifications: Update	update	Alert system report updated
SYSTEM-INIT	System: Initialization	info	System initialized with user <username>
TEAM-ADDMEMBER	Teams: Add user	create	User <userid> has been added for team <teamid>
TEAM-CREATE	Teams: Add	create	Team <teamid> has been created
TEAM-DELETE	Teams: Delete	delete	Team <teamid> has been deleted
TEAM-REMOVEDMEMBER	Teams: Remove user	delete	User <userid> has been removed from team <teamid>
TEAM-SHARE	Teams: Share	update	Team <teamid> has been shared with company <companyid>
TEAM-UNSHARE	Teams: Unshare	update	Team <teamid> has been unshared with company <companyid>
TEAM-UPDATE	Teams: Edit	update	Team <teamid> has changed name to <newname>
USER-ADD	User: Add	create	<firstname>.<lastname> with user id <userid> has been created.
USER-EMAIL	User: Email invitation	info	Invitation (email) has been sent to user with user-id <userid>

Continued on next page

Table 2 – Continued from previous page

Event ID	Description	Type	Details
USER-IMPORT	User: Excel import	create	An excel file has been imported
USER-MANUAL	User: Manual invitation	info	Invitation (manual) has been sent to user with user-id <userid>
USER-REMOVE	User: Delete	delete	User <userid> has been deleted.
USER-REVOKE	User: Revoke access	delete	User <userid> has revoked access.
USER-SMS	User: SMS invitation	info	Invitation (sms) has been sent to user with user-id <userid>
USER-UPDATE	User: Update	update	Userid <userid> has teams set to following: <list of team ids>
USER-UPDATE	User: Update	update	Userid <userid> has been removed from following teams: : <list of team ids>
USER-UPDATE	User: Update	update	Userid <userid> set emergency lists to following: <list of emergency ids>
USER-UPDATE	User: Update	update	Userid <userid> has removed following emergency lists: : <list of emergency ids>
USER-UPDATE	User: Update	update	User id <userid> updated to following: <list of metadat>.
USER-UPDATE	User: Update	update	Userid <userid> updated image.
USER-UPDATE	User: Update	update	Userid <userid> updated groups

C Version history

Ver.	Author	Date	Notes
1.0	SS	31-08-2020	Initial version in \LaTeX based on DSS4.3.1
1.1	SS	15-12-2020	Updated to apply full version numbering.
1.2	AG	12-03-2021	Added "Apps" sections.
1.3	KK	23-02-2022	Revamped language and updated screenshots.