

Dencrypt Communication Solution

Operational User Guide

Dencrypt Server System 5.4.0

v.1.3



6 February 2023

Public

Contents

| Pr | oduct | versions | 4 |
|----|------------|--|----|
| 1 | Intro | oduction | 4 |
| | 1.1 | Content | 4 |
| | 1.2 | System architecture | 5 |
| | 1.3 | Operational modes | 6 |
| | 1.4 | Authenticated connections | 6 |
| 2 | Secu | irity 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 |
| - | D I | | 45 |
| 3 | Phor | nedook | 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 |

| v.1 | .3 | Public | DENCRYP | Τ |
|-----|------|--|----------------|----|
| | 3.5 | Example 2: Contact groups representing hierarchy | | 21 |
| | 3.6 | Recommendations | | 21 |
| 4 | Tear | ns | | 23 |
| 5 | Eme | rgency contacts | | 23 |
| - | | | | |
| 6 | Den | crypt 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 | Fund | ctionality 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 | 8.3 Adva | Examples | 77 80 |
| A | 8.3 Adva A.1 | Examples | 77 80 80 |
| A | 8.3 Adva A.1 A.2 | Examples | 77 80 80 81 |
| A | 8.3 Adva A.1 A.2 A.3 | Examples | 77 80 80 81 81 |
| A | 8.3 Adva A.1 A.2 A.3 A.4 | Examples | 77 80 81 81 83 |
| A | 8.3 Adva A.1 A.2 A.3 A.4 A.5 | Examples | 77 80 81 81 83 83 |
| A | 8.3 Adva A.1 A.2 A.3 A.4 A.5 A.6 | Examples | 77 80 81 81 83 83 84 85 |
| A | 8.3 Adva A.1 A.2 A.3 A.4 A.5 A.6 A.7 | Examples | 77 80 81 81 83 83 84 85 86 |
| A | 8.3 Adva A.1 A.2 A.3 A.4 A.5 A.6 A.7 A.8 | Examples | 77 80 81 83 83 84 85 86 88 |
| A | 8.3 Adva A.1 A.2 A.3 A.4 A.5 A.6 A.7 A.8 A.9 | Examples Anced management functions Change of operational mode Dencrypt Control Center: Configuration Dencrypt Certificate Manager: Configuration Dencrypt Provisioning Server: Configuration Dencrypt Database: Configuration Dencrypt Communication Server: Configuration Dencrypt System Bridge: Configuration Features configuration SSH access | 77 80 81 81 83 83 84 85 86 88 88 89 |
| В | 8.3 Adva A.1 A.2 A.3 A.4 A.5 A.6 A.7 A.8 A.9 Audi | Examples | 77 80 81 83 83 84 85 86 88 88 89 90 |



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 endusers, 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.

| ♦ Home | | - | | | |
|--------------------|-------------|--------------|---------------|---------------|---|
| | | - C | My Company | ~ | |
| Lusers | | Show 25 II | sers per page | | |
| 🚢 Groups | L+ New User | 0.0007200 | | Search Q | |
| 🖬 Teams | Select All | First Name 🔺 | Last Name | Status Connex | Z |
| Emergency Contacts | | Brian | Davis | Registered | |
| Departments | | James | Skinner | Created | |
| Import | | Michael | Todd | Created | |
| Notifications | | | | | |
| TATISTICS • | | | | | |
| YSTEM | | | | | |

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.

| O Dencrypt Control Center | | | | × | ⊖ Admin_userguide + |
|---------------------------|----------------------|---|---|----------|---------------------|
| 😤 Home | | ¥ Delete user data | Delete user data | | |
| ADMINISTRATION - | | × Delete log records | Delete log records | | |
| Lusers | Brian Davis | ✓ Deactivate all devices | Remove all devices' access | | |
| 🖀 Groups | i Info | Deactivate 🛇 | Delete 🗊 | Search Q | |
| I Teams | C Details | User has lost his device(s) or no longer trusted | User should no longer should be part of the system | | ß |
| Emergency Contacts | 😂 Groups | | | | |
| A Departments | Teams | | | | |
| -B Import | C Emergency Contacts | | | | |
| A Notifications | Devices | | | | |
| STATISTICS > | M Invite | | | | |
| SYSTEM > | → Transfer | | | | |
| | × Remove | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |



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-installatio n/import-and-export-certificate-microsoft-windows
 - MacOS: https://www.sslsupportdesk.com/how-to-import-a-certificate-into-m ac-os/

| Dencrypt Control Co | enter | Admin_userguide |
|------------------------|--|-----------------|
| A Home | Add this certificate to your browser's trusted CA list | |
| ADMINISTRATION > | This will verify the server upon future visits: | |
| STATISTICS . | Secure https:// | |
| SYSTEM - | Download As File | |
| | BEGIN CERTIFICATE | |
| n Browser Verification | MIIFxTCCA62gAwIBAgIJAOCk+PFy40VMMA0GCSqGSIb3DQEBDQUAMG4xCzAJBgNV | |
| | BAYTAkRLMRMwEQYDVQQHDApDb3B1bmhhZ2VuMRUwEwYDVQQKDAxEZW5jcn1wdCBB | |
| Password Policies | cFMxFDASBgNVBAMMC2RlbmNyeXB0LmRrMR0wGwYJKoZIhvcNAQkBFg5pdEBkZW5j | |
| | cnlwdC5kazAeFw0xNjEwMTMxNzE4MzNaFw0yNjEwMTMxNzE4MzNaMG4xCzAJBgNV | |
| | BAYTAKRLMRMwEQYDVQQHDApDb3B1bmhhZ2VuMRUwEwYDVQQKDAxEZW5jcn1wdCBB | |
| | CFMXFDASBgNVBAMMC2RIbmNyeXB0LmKrMK0wGwYJKoZIhvCNAQkBFg5pdEBkZW5j | |
| | Chiwdc5kazCCA11wDQYJKOZINVCNAQEBBQADggIPADCCAgoCggIBAJgso7P11nJ4 | |
| | CUC/VCVTy15HTerV64ThBpTc65XhrRXa0FX25QWK5135SQdedQeGrXTFJ5W726T2 | |
| | LASAGeren BLV(3)-WECKHOCE, TDBB7006 (7H)-Y (BETMDSES7EDB1E07 (UEDTEE)) (| |
| | TZol 3pT4FPuPoELEWDP1Db2C201770KX/biiInD3132EF011QF111D1C32W/ | |
| | OvalkTEp/sPiedPibnHvaG/a3k010i678aviTchELt7Ube04ubRu6kTELUTa0aE3 | |
| | To 14E4u0dfW146vrv0B1m0a9/gs70musnWi5Ke8a4v/U4vnnvs8D+7vsDUan83sr | |
| | a6wgJZDg3SjWoKvkv4utVZga0zPvGB2P9NjillsMk2BxDrg8KK/8ESf8TL4kYkcO | |
| | 3GYILBIApTLCa8YvUuH3dXYIFJ4elX8twHRcwT/Fd0Xe4pf5vJk1rm9oHilgFvuC | |
| | CrpWa0esdWVGct312RAKvF36diGMuWsEeDOMALHuZDziubHI7DtOwKaoZeKUnnnF | |
| | Njt9SQXL9dwHjQdWis7hyjD/+IGfJOwr41zYscbjKZhXjH0miEwwU9BZLfDzsYDe | |
| | +Tr+nKRbx+SoRGBUTwhsrbvwlQAIfj9RAgMBAAGjZjBkMB0GA1UdDgQWBBSxMuTE | |
| | C3eXJSqhpOHh7V4Pmf6jGzAfBgNVHSMEGDAWgBSxMuTEC3eXJSqhpOHh7V4Pmf6j | |
| | GzASBgNVHRMBAf8ECDAGAQH/AgEBMA4GA1UdDwEB/wQEAwIBBjANBgkqhkiG9w0B | |
| | AQ0FAAOCAgEAQTQhGPuwLotf2zTNWjky8DSdjueuSa6pu/xBX2AR84WVbBebY39G | |
| | L5yF5lIU0FVn048PaS4P0sAlsdsjs0baWZk4onnE97FjqctespIyFy16Y7vLUPiq | |
| | EDcGcIW7SYriUyi2xQ+LvTVPnFi5cU97cYN/KkhWVm+vNCJJXUC9TYzuza/gU97P | |
| | kf102hzngDG2WKUd4txwrbm6VBwR9PpHaJIMG8iHiJtyxUV5VCEgL6ME9pSe3kA3 | |
| | ZNVtNpnjkq8X15hk0oWdlEccywcKThJGvWKQDjDW8/4jMh0TmiErPBKmBT52hNjh | |
| | 4wZBMN7wAn99B1VlQfqZfgLqTuYWr9U1m4NubK7GEtpEH14vEyPjVaMs4kLmb1cQ | |
| | msgBjzsmDXyudm0Sa79wxFFganpIKnBuLj86Wx6A19kzA4/7tiGAJxFZkqEDWQhD | |
| | XBUZAPMhnZB0rOLvExwUZXmLcxBjAKVydVd1slHPicjwyHoID/07TrSJdWL7uXM6 | |
| | 0AqHXs+OQjobvMgAqfFNK8WD/Q80+gi8bvWfhf5Fn+3NoOR9gcrNRJ/kba4wsytM | |
| | epquM8bQXAz+yjwjGEvXXhYXRNFy82OK1SRBm+wKV6D3d5MRlzlh3aHOrWKltnNd | |
| | 9zn6jUgOWWHHM36q3wMnULiECo6Lzj6uEG0/x5JWvUr47Rbsy8/G0K4= | |

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 | 9 | 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 intergroup 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.

| Sten 1 | Onen | Administration | -> | llsprs |
|---------|------|----------------|----|--------|
| JUCP I. | Open | Aummistiution | ~/ | USEIS. |

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.



| - | | | | × |
|--------------------|--------------------------------|-----------|---|---|
| Home | Group info | | Link to other groups | |
| MINISTRATION - | Name | | My Company - Shared | |
| Users | Employee | Save Name | - my company - charca | _ |
| Groups | Company | | Director | |
| Teams | My Company | | Dismiss 🔺 | |
| Emergency Contacts | Members can contact each other | | | |
| Departments | Members | | Members | |
| Import | James Skinner | | Brian Davis | |
| Notifications | Michael Todd | | Michael Todd | |
| TISTICS | | | | |
| STEM | | | | _ |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

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.



| O Dencrypt | Control Center | | e iei - |
|-------------------|--------------------------------|-----------------------------------|---------|
| 😤 Home | Group info | Link to other groups | |
| ADMINISTRATION - | Name | = My Company Shared | |
| Lusers | Group 2 🖬 Sa | ve Name | |
| 🚢 Groups | Company | Group 1 | |
| Teams | My Company | | |
| D Emergency Con | Members can contact each other | ECHO_Connex_MSG_Bridge - Unshared | |
| The Departments | Members | | |
| Companies | Brian Davis | | |
| -Si Import | James Skinner | | |
| A Notifications | | | |
| Lo Administrators | | | |
| TATISTICS • | | | |
| SYSTEM . | | | |
| | | | |
| | | | |
| | | | |
| | | | |

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.

| SLED I: ODELLAULILIUSTICUUL-> OLOUDS | 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.



| Dencrypt Cont | trol Center | | | Admin_userguide |
|--------------------|--------------------------------|-----------|---|-----------------|
| Home | Group info | | Link to other groups | ^ |
| MINISTRATION - | Name | | | |
| | Employee | Save Name | My Company - Shared | |
| Groups | Company | | Director | |
| | My Company | | | |
| Teams | | | Other Company - Unshared | |
| Emergency Contacts | Members can contact each other | | | |
| Departments | Members | | | |
| Import | James Skinner | | | |
| Notifications | Michael Todd | | | |
| TISTICS . | | | | |
| TEM • | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | Delete Group | | | |

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.

| O Dencrypt Contr | ol Center | | | O Admin alpha * | O Dencrypt Contro | ol Center | | | e Admin-alpha * |
|---|---|-----------|----------------------|-----------------|---|--|----------|---|-----------------|
| Hone ADMINISTRATION → ADMI | Group info Name Convergent Competing Africa Competing Africa Competing Africa Competing Africa Members An remoters Dense Group | Size Name | Link to other groups | × | Aounistantos Aounistantos Aounistantos Aounistantos Aounistantos Alexandres Alexan | Group info Nerre Grane Corputy Company Alters Corputy Company Alters Nerrebers Nerrebers Deteste Group | Sov Nure | Link to other groups Company Agina - Shand Company Agina - Shand Company Samo - Shafkard | |

(a) Example 1: Development group settings.

(b) Example 1: Sales group settings



| O Dencrypt Contro | gl Center | | | 🖯 Admin-alpha * | O Dencrypt Contr | ol Center | | | O Admin-alpha + |
|---|---|-------------|---|------------------|---|--|-------------|--|-----------------|
| Annovember Control Annovember Contro | Context Group Info Nave Unropey Context Adva Workson can sense and wher Members Re newtors | D Sare None | Link to other groups Company Apla-Stand Company Apla-Stand The Company Bran-Stand Company Bran-Stand Resources | • Anomograv X | Conscript Contr more Conscript Control Control Conscript Control Contro Control Contro Control Control Control Con | Group info mer mer Comme | C Sove Name | Link to other groups • Corputy Stave-Staved By prove sharef • Corputy Alan-Staved • Corputy Alan-Staved • Corputy Alan-Staved • Corputy Alan-Staved • Corputy Stave-Staved • Corputy Stave-Sta | 0 Januarya X |
| | Delete Group | | | | | Delete Group | | | |

(a) Example 1: Management 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:

- (a) **Standard** No additional links required.
- (b) **VIP** Apply an OUT link to **Standard**.
- (c) **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 hierachy.

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 priviligies.

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 \rightarrow 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].

| O Dencrypt Control Center | | | | | | Θ | Admin-demo |
|---------------------------|---------------------------|--------------------------|--------------------------------|------|------------------------|--------------------------|---------------------------|
| A Home | | | | | laet | | |
| ADMINISTRATION . | System ID | System Name | DNS | Port | Updated | State | Action |
| STATISTICS • | bravo.dss.dencrypt.local | bravo.dss.dencrypt.local | dsb01.bravo.dss.dencrypt.local | 443 | 2021-05-25 | Active | ۰ چ |
| SYSTEM - | | | | | Connection | | |
| M Browser Verification | Remote System ID | | | | ← Sync Da → Sync Da | ta (Remot ta (Local t | e to Local) to Remote) |
| Password Policies | Your System | | | | Check C | onnection | 1 |
| Licenses | System ID: echo.dss.den | crypt.local | | | Configuration | onnectior | n Request |
| E Custom Attributes | System Name: echo.dss. | dencrypt.local | | | Export C | onnectior | n Request |
| Standard Messages | Port: 443 | ur DSP's configuration | | М | Delete | | _ |
| 🖺 Logs | Change trese settings you | a DSD's configuration | | | | | |
| Certificates | | | | | | | |
| Apps | | | | | | | |
| Servers | | | | | | | |
| 𝔄 Bridges | | | | | | | |
| Features | | | | | | | |
| Alerts | | | | | | | |
| C Backup | | | | | | | |

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 trigged 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.



| O Dencrypt Control Cen | ter | | ⊖ admin - |
|-------------------------|-------------|-----------------------|-----------|
| ☆ Home ADMINISTRATION ▼ | | Company My Company | |
| Lusers | + New Group | | |
| 🐣 Groups | Group Name | Members | |
| Teams | My Group | 1 | |
| Emergency Contacts | | | |
| Lepartments | | | |
| E Companies | | | |
| - Import | | | |
| Lo Administrators | | Error Add Grou | un X |
| STATISTICS • | | | a p |
| SYSTEM . | | | |

Figure 18: Where to click to show error details.

| O Dencrypt Control | Center | ⊖ admin - |
|--------------------|---|-----------|
| 🖀 Home | Company My Company | |
| ADMINISTRATION - | Untitled - Google Chrome – 🗆 🕺 | _ |
| Lusers | ① about:blank | |
| 🐣 Groups | An error occured Group.py line 218. No variable named: 'user' | |
| Teams | | _ |
| Emergency Contacts | | |
| 击 Departments | | |
| Companies | | |
| -S Import | | _ |
| Administrators | Error Add Group | × |
| STATISTICS • | | |
| SYSTEM ► | | |

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 logins 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].



| O Dencrypt Control Center | |
|---------------------------|--|
| Username | |
| Password | |
| Login | |

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.

| O Dencrypt Control Cer | iter | | | O Admin-de |
|----------------------------|-------|-------|-------|------------|
| 谷 Home | | | | |
| ADMINISTRATION > | DCC | DCM01 | DPS01 | DDB01 |
| STATISTICS . | V DCC | DCM | V DPS | V DDB |
| DVOTELA | ОК | ок | ок | ок |
| STSTEW . | DCS01 | DCS02 | DMS01 | |
| | V DCS | DCS | V DMS | |
| | ОК | ОК | ОК | |

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 Center

| Dencrypt Control Cente | r | | | Dencrypt-k |
|------------------------|------------------|-------|------------------|--------------------------------------|
| A Home | | | | Change Password |
| DMINISTRATION . | dcc01 | dcm01 | dps01 | REST API |
| TATISTICS | V DCC | 🗸 рсм | V DPS | |
| TATISTICS F | ОК | ОК | ОК | 5.4.0-milestone-dss-5.4.0-7acbc600+1 |
| YSTEM • | dcs01 | dcs02 | dsb01 | |
| | DCS | 🗸 dcs | DSB | |
| | High memory load | ОК | High memory load | |

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.

| O Dencrypt Control Ce | Admin-dem | |
|-----------------------|------------------------|--|
| A Home | liser Adminutance | |
| DMINISTRATION . | Role: Service Access | |
| TATISTICS • | Change Password | |
| SYSTEM 🕨 | Current Password | |
| | New Password | |
| | Repeat New Password | |
| | 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 \rightarrow 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.

| Dencrypt Control Center | | | | | O Admin_userguide |
|-------------------------|-------------|--------------|--------------------------|---------------|-------------------|
| Home | | | Company | | |
| MINISTRATION - | | | My Company | ~ | |
| Users | | | | | |
| Groups | L+ New User | | Show 25 users per page V | Search O | |
| Teams | Select All | First Name 🔺 | Last Name | Status Connex | Ľ |
| Emergency Contacts | | Brian | Davis | Registered | |
| Departments | | James | Skinner | Created | |
| Import | | Michael | Todd | Created | |
| Notifications | | | | | |
| ATISTICS . | | | | | |
| STEM . | | | | | |

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: | |
|---------------------|--|
| First and last name | Name of the user as it appears in the phonebook. |
| Email address | Email address for receiving the invitation email for pro- visioning. |
| Phone number | Phone number for receiving the invitation SMS for provi- |
| | sioning (if SMS provisioning is enabled by the same sys- |
| | tem). The flag indicates the country code. |
| Company | (Prefilled) Used for grouping users in the phonebook. |
| Department | Used for subgrouping users within a company. |
| Title | The title of the user at it appears in the phonebook. |
| Image | Loads an avatar image. If left blank, the company logo is applied. |
| Groups | 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.



| O Dencrypt Control Cente | ər | | | \varTheta Admin-demo 🕶 |
|--------------------------|------------------|----------------------------------|---------------------------|------------------------|
| 脅 Home | 2 | User | 📇 Groups | × |
| | st Name | Last Name | Group 1 | |
| Aller | A Pirst Name | A Last Name | Group 2 | |
| Em. | ail | Phone number | | |
| 🛎 Groups | Email | Phone number | | |
| Teams Cor | mpany | Department | | |
| Contacts | My Company | Department A 🛛 🗘 | | |
| Title | e | Image | | |
| Companies | Title | Choose Image | Phone book | |
| B Import | | | Brian Davis | |
| Use | er ID (Optional) | Password (Optional) | My Company Department A | |
| A Notifications | Autogenerate | Autogenerate | James Skinner | |
| 20 Administrators | | | Michael Todd | |
| STATISTICS . | | | My Company Department A | |
| SYSTEM . | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | Create User | |

Figure 25: Create a new user.

7.6.3 Display user details

Display user details

| Step 1: | I: 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.

v.1.3



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

Outputs:

• The user details are modified.

| O Dencrypt Contro | ¢ | | | Admin-demo + |
|----------------------|--------------------|--|-----------------|--------------|
| A Home | | First Name | Last Name | |
| | | A Brian | A Davis | |
| Lusers | Brian Davis | Email | Phone number | |
| têt Groupo | | e brian@mycompany.com | 12 34 56 78 | |
| - Groups | i Info | Company | Department | |
| III Teams | C Details | My Company | Department A \$ | onnex 🕑 |
| D Emergency Contacts | 🖶 Groups | Title | User ID | a |
| A Departments | III Teams | • | b.dk2r8o8c1 | lay |
| Companies | Emergency Contacts | Image | | 4 |
| -B Import | Devices | Use Company Logo Custom Image | | |
| Notifications | S Invite | | Reset 🕞 Save | |
| 20 Administrators | → Transfer | | | |
| STATISTICS . | × Remove | | | |
| SYSTEM . | | | | |
| | | | | |

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.

| O Dencrypt Control C | | | | Admin-demo • |
|----------------------|--------------------|----------|-----------------------------------|--------------|
| 😤 Home | *** | 📇 Groups | E Phone book | |
| ADMINISTRATION - | 2 Lisers | Group 1 | Cannot display for multiple users | |
| 💄 Users | 2 00010 | Group 2 | | |
| as Groups | i Info | Group 3 | | |
| Teams | 🖉 Details | | | |
| S Emergency Contacts | 📇 Groups | | | |
| - Departments | Teams | | Reset 🖬 Save | |
| Companies | Emergency Contacts | | | |
| -5 Import | Devices | | | |
| Notifications | Market Invite | | | |
| Lo Admi | → Transfer | | | |
| STATISTIC | × Remove | | | |
| SYSTEM I Info | | Martin | Smith Created | |
| Detelle | | | | |



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.

| O Dencrypt Control C | | | | e Admin-demo - |
|----------------------|----------------------|--------|--------------|----------------|
| 番 Home | | Teams | | |
| ADMINISTRATION - | | Team 1 | | |
| 💄 Users | Brian Davis | Team 2 | | |
| 🛎 Groups | i Info | | | 2 |
| Teams | 🕑 Details | | | ď |
| Emergency Contacts | 📽 Groups | | | |
| 🖧 Departments | 📅 Teams | | | |
| Companies | D Emergency Contacts | | | |
| -🖺 Import | Devices | | | |
| A Notifications | Invite | | | |
| Lo Administrators | → Transfer | | | |
| STATISTICS . | × Remove | | | |
| SYSTEM | | | | |
| | | | | |
| | | | Reset 🖬 Save | |
| | | | | |

Figure 30: Allocate users to teams.

| | | | | 🗙 🕒 Admin-demo 👻 |
|--------------------|----------------------|------------|------------|------------------|
| A Home | | Teams | | |
| ADMINISTRATION - | 2 Users | Team 1 | | |
| 💄 Users | | X Team 2 | | |
| 🛎 Groups | i Info | + New Team | | 2 |
| Teams | 🕑 Details | | | |
| Emergency Contacts | 🖶 Groups | | | |
| 🚠 Departments | 📅 Teams | | | |
| Companies | D Emergency Contacts | | | |
| -S Import | Devices | | | |
| Notifications | Invite | | | |
| 2 Users selected | → Transfer | | | |
| STATISTIC Cancel | × Remove | | | |
| SYSTEM | | | | |
| C Details | | | | |
| 😤 Groups | | | Reset Save | |



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.

| O Dencrypt Control O | | | | Admin- | demo v |
|----------------------|--------------------|------------------|--|--------|-------------------|
| 😤 Home | | Emergency Lists | | | |
| ADMINISTRATION - | | Emergency list 1 | Anne Harris My Company Department A | | |
| 🚨 Users | Dean Williams | | Brian Davis My Company Department A | | |
| 🖀 Groups | i Info | | | 2 | |
| Teams | 🕑 Details | | | ß | |
| Emergency Contacts | 44 Groups | | | | |
| A Departments | Teams | | | | |
| Companies | Emergency Contacts | | | | |
| -5 Import | Devices | | | | |
| A Notifications | S Invite | | | | |
| 20 Administrators | → Transfer | | | | |
| STATISTICS . | × Remove | | | | |
| SYSTEM . | | | | | |
| | | | Reset | Save | |

Figure 32: Allocate users to emergency lists.

| | 1 | | | Admin-demo 🕶 |
|-----------------------|--------------------|------------------|--|--------------|
| 番 Home | :•• | Emergency Lists | | |
| ADMINISTRATION - | 3 Lisers | Emergency list 1 | Lorelai Marvinson My Company Department A | |
| 🚨 Users | 0 00010 | Emergency list 2 | | |
| A Groups | i Info | | | |
| Teams | 🖉 Details | | | |
| Emergency Contacts | 🛎 Groups | | | |
| Departments | Teams | | | |
| Companies | Emergency Contacts | | | |
| -5 Import | Devices | | | |
| A Notifications | S Invite | | | |
| Admi 3 Users selected | → Transfer | | | |
| STATISTIC Cancel | × Remove | | | |
| SYSTEM | | | | |
| C Details | | | _ | |
| a Groups | | | Reset 🖬 Sa | ave |



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 | |
|---------------------|--|
| ClientId | Device specific application id. |
| Application | Application name. |
| Device | Manufacturer and device model. |
| Operating system | OS type and version. |
| Created | Timestamp for device creation in the system. |
| Last Registration | Timestamp for the last successful connection to the sys- |
| | tem. |
| Push tokens | |
| Certificate | Certificate name for push token. |
| Capability | Related push service. |
| Encryption | Support for content encryption. |
| Client certificate | |
| Status | Certificate status: Valid, Expired or Revoked. |
| Serial | Certificate serial number. |
| Created | Timestamp for creation. |
| Expiry | Expiry date. |

Outputs:

• Display of device data.

| O Dencrypt Control Center | | | | | × |
|---------------------------|-------------|----------------------|---|------------------|-------|
| -∰ Home | | | | | |
| ADMINISTRATION * | | | DESKTOP-SB78NBF [Connex Desktop] | | |
| 🛓 Users | | Brian Davis | | | |
| 4월4 Groups | 2+ New User | 1 Info | [] Iphone09's iPhone (Connex) | | |
| Tearra | Select All | @ Denais | This device is deactivated | O Reactivate | annex |
| Emergency Contacts | | 4 Groups | Info | | |
| A Departments | | Tearro | Clientid 4859e018-crist-9658-5c58- | Active the 75x15 | |
| a import | | C Emergency Contacts | Application Connex 6.4.0 | | |
| Notifications | | D Devices | Device apple iPhone SE (GSM) | | |
| STATISTICS . | | a inste | Operating System ios 15.7 | | |
| SYSTEM . | | → Transfer | Created 2023-02-01 12:52 | | |
| | | × Bemave | Last Connected 2023-02-01 12:52 | | |
| | | | Last Deactivated 2023-02-01 13:32 | | |
| | | | Push Tokens | | |
| | | | Certificate Capability | Encryption | |
| | | | com.dencrypt.tngStore - production apple-back | ground Yes | |
| | | | com.dencrypt.tngStore - production apple-mes | sage Yes | |
| | | | com.dencrypt.tngStore - production apple-volp | Yes | |
| | | | Client Certificates | | |
| | | | Status Serial Created | Expiry | |
| | | | Revoked 462 2023-02-01 12:52 | 2025-01-01 12:52 | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

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.

| O Dencrypt Control C | | | Admin-demo 🕶 |
|----------------------|--------------------|--|--------------|
| A Home | | Application | |
| ADMINISTRATION - | Dean Williams | | |
| 🛎 Groups | i Info | | |
| Teams | 🕑 Details | | ß |
| Emergency Contacts | 🛎 Groups | | |
| # Departments | Teams | Method | |
| Companies | Emergency Contacts | | |
| -Di Import | Devices | Email SMS QR Code Link | |
| Notifications | S Invite | | |
| Administrators | → Transfer | | |
| STATISTICS . | × Remove | Verify | |
| STOLEM | | Send Connex invitation through Dean@dencrypt.dk to Dean Williams | |
| | | | |
| | | Reset 🛃 In | vite |

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.



| O Dencrypt (| | | | Admin-demo - |
|-------------------|----------------------|----------------|------------|--------------|
| A Home | \cap | New Company | | |
| | | Select Company | - \$ | |
| 💄 Users | Dean Williams | New Department | ¢ | |
| Croups | i Info | | → Transfer | |
| III Teams | 🗹 Details | | | Ľ |
| Emergency Cont | 😫 Groups | | | |
| Departments | III Teams | | | |
| Companies | D Emergency Contacts | | | |
| -M Import | Devices | | | |
| A Notifications | Invite | | | |
| Lo Administrators | → Transfer | | | |
| STATISTICS > | × Remove | | | |
| SYSTEM . | | | | _ |

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.

| O Dencrypt Control Center | | | | Admin_userguide + |
|---|---|--|--|-------------------|
| # Home ADMINISTRATION | Brian Davis | X Delete user data X Delete log records ✓ Deactivate all devices | ✓ Delete user data ✓ Delete log records ✓ Remove all devices' access | |
| Croups Teams Emergency Contacts Departments Import Notifications | i Info d' Details de Groups T Teams de Emergency Contacts D Devices | Deactivate 📎 User has lost his device(s) or no longer trusted | Detete () User should no longer should be part of the system | Steerin Q. |
| STATISTICS > SYSTEM > | ➡ Transfer ★ Remove | | | |
| | | | | |

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 \rightarrow 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.

| O Dencrypt Control Cer | ter | | O Admin-demo 🕶 |
|------------------------|-------------|------------|----------------|
| 송 Home | | Company | 1 |
| ADMINISTRATION - | | My Company | \$ |
| Lusers | | _ | |
| 🚢 Groups | + New Group | | |
| Teams | Group Name | Members | |
| Emergency Contacts | Group 1 | 2 | |
| Lepartments | Group 2 | 3 | |
| D Companies | Group 3 | 0 | |
| - Import | | | |
| A Notifications | | | |
| Lo Administrators | | | |
| STATISTICS • | | | |
| SYSTEM • | | | |

Figure 38: Frontpage for contact groups management.

7.7.1 Create a new Group

Create new contact group

- Step 1: Open Administration \rightarrow 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.



| O Dencrypt Control Center | | | × | | e Admin-demo - |
|---------------------------|-------------|--------------|--------------|----|----------------|
| A Home | | + New Group | | | |
| ADMINISTRATION - | | Name | | \$ | |
| Lusers | | A Group Hame | | | |
| 🖶 Groups | + New Group | | Create Group | | |
| Teams | Group Name | _ | | | |
| Emergency Contacts | Group 1 | | 2 | | |
| - Departments | Group 2 | | 3 | | |
| Companies | Group 3 | | 0 | | |
| - Import | | | | | |
| A Notifications | | | | | |
| 20 Administrators | | | | | |
| STATISTICS > | | | | | |
| SYSTEM • | | | | | |

Figure 39: Create new contact group.

7.7.2 Edit and linking contact groups

Edit and linking contact groups

- Step 1: Open Administration \rightarrow 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.

| O Dencrypt Contr | ol Center | | | e Admin_userguide - |
|--------------------------|--------------------------------|-----------|-----------------------|---------------------|
| A Home | Group info | | Link to other groups | × |
| ADMINISTRATION - | Name Employee | Save Name | ▼ My Company - Shared | |
| A Groups | Company Mr. Company | | Director | |
| Teams Emergency Contacts | Members can contact each other | | | |
| Departments | Members | | Members | |
| -🖺 Import | James Skinner | | Brian Davis | |
| A Notifications | Michael Todd | | Michael Todd | |
| STATISTICS . | | | | J |
| SYSTEM . | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | Delete Group | | | |
| | | | | |

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 \rightarrow Teams.

Step 2: Select the company from the dropdown menu.

Parameters: Company Selected company

| O Dencrypt Control Cente | ər | | O Admin-demo 🕶 |
|--------------------------|------------|------------|----------------|
| 😤 Home | | Company | |
| ADMINISTRATION - | | My Company | \$ |
| Lusers | | _ | |
| 🛎 Groups | + New Team | | |
| Teams | Name | Members | |
| S Emergency Contacts | Team 1 | 0 | |
| Departments | Team 2 | 1 | |
| Companies | | | |
| -🖪 Import | | | |
| A Notifications | | | |
| 20 Administrators | | | |
| STATISTICS • | | | |
| SYSTEM • | | | |

Public



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.



| O Dencrypt Control Center | | | V. | O Admin-demo - |
|---------------------------|------------|------------|----|----------------|
| A Home | | + New Team | ^ | |
| ADMINISTRATION - | | Name | | \$ |
| Lusers | | A Name | | |
| 🚢 Groups | + New Team | Create Te | am | |
| 🔝 Teams | Name | | | |
| Emergency Contacts | Team 1 | 0 | | |
| - Departments | Team 2 | 1 | | |
| I Companies | | | | |
| -🛅 Import | | | | |
| A Notifications | | | | |
| Lo Administrators | | | | |
| STATISTICS . | | | | |
| SYSTEM > | | | | |

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.

| O Dencrypt Control C | Center | | | × | e Admin-demo ▼ |
|----------------------|--|-----------|--|-----|----------------|
| 😤 Home | Team | | Available | ^ | |
| ADMINISTRATION - | Name | | Selected companies will may add team members | _ | |
| 🚨 Users | Team 1 | Save Name | My Company | | |
| A Groups | The name is shown to all team members Company | | ECHO_Connex_MSG_Bridge | | |
| Teams | My Company | | | | |
| Emergency Contacts | Members | | | | |
| - Departments | Go to users to add or remove users to the team | | | _ | |
| Companies | Brian Davis My Company Department A | | | | |
| -5 Import | Dean Williams | | | | |
| A Notifications | My Company Department A | | | | |
| 20 Administrators | James Skinner My Company Department A | | | - 1 | |
| STATISTICS > | Jess Davidson My Company Department A | | | - 1 | |
| SYSTEM . | | | | | |
| | Delete Team | | | | |



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 \rightarrow Emergency Contacts.

Step 2: Select the company from the dropdown menu.

Parameters: Company Selected company

| O Dencrypt Control Cen | ter | | 🕒 Admin-demo 👻 |
|------------------------|----------------------|------------|----------------|
| A Home | | Company | |
| ADMINISTRATION - | | My Company | \$ |
| 🚢 Users | | | |
| ^ය Groups | + New Emergency List | | |
| 🔝 Teams | Name | Users | |
| Emergency Contacts | Emergency list 1 | 2 | |
| 🖧 Departments | Emergency list 2 | 1 | |
| I Companies | | | |
| -🛅 Import | | | |
| Notifications | | | |
| 20 Administrators | | | |
| STATISTICS . | | | |
| SYSTEM . | | | |

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.



| O Dencrypt Control Center | | × I | O Admin-demo ▼ |
|-----------------------------|------------------|--------------------|----------------|
| A Home | | New Emergency List | |
| ADMINISTRATION - | N | lame | \$ |
| Lusers | | A Name | |
| 🚢 Groups | + New Emergenc | Create List | |
| Teams | Name | | |
| Distance Emergency Contacts | Emergency list 1 | 2 | |
| rt Departments | Emergency list 2 | 1 | |
| Companies | | | |
| -🗗 Import | | | |
| A Notifications | | | |
| Lo Administrators | | | |
| STATISTICS > | | | |
| SYSTEM > | | | |



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:

NameIdentifier for emergency lists.ContactsUsers allocated to the list.

Outputs:

• Updated user allocations to an emergency list.

| O Dencrypt (| Control Center | | | ⊖ Admin-demo × |
|-------------------|--|-----------------|--|---------------------------|
| A Home | Emergency list | | Available to | ^ |
| | Name | | Users of these companies may have their emergency contacts set to this | list |
| Lusers | Emergency list 1 | Save Name | ECHO_Connex_MSG_Bridge | |
| 🎎 Groups | Company My Company | | BRAVO_Connex_MSG_Bridge | |
| Teams | | | My Company | |
| Emergency Cont | Contacts | | | · |
| - Departments | These users will be contacted when users assigned to this emergency functionality | s list triggers | | |
| Companies | Name | | | |
| -🛅 Import | Type name of user to be added | × | | |
| Notifications | Anne Harris | | | |
| 20 Administrators | My Company Department A | | | |
| STATISTICS > | Brian Davis My Company Department A | × | | |
| SYSTEM > | | | | |
| | Delete 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 \rightarrow Departments.

Step 2: Select the company from the dropdown menu.

Parameters: Company Selected company

| O Dencrypt Control Cen | ter | 🕒 Admin-demo 🕶 |
|------------------------|------------------|----------------|
| 쑭 Home | Company | |
| ADMINISTRATION 👻 | My Company 🗘 | |
| 🚨 Users | | |
| 🔐 Groups | + New Department | |
| Teams | Department Name | |
| Emergency Contacts | Department A | |
| 🕂 Departments | | |
| I Companies | | |
| -🖺 Import | | |
| A Notifications | | |
| Lo Administrators | | |
| STATISTICS • | | |
| SYSTEM . | | |

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.



| O Dencrypt Control Center | | | | | O Admin-demo 🕶 |
|---------------------------|-----------------|-------------------|---|---|----------------|
| 😤 Home | | + New Department | × | | |
| ADMINISTRATION - | | Name | | ÷ | |
| Lusers | | A Department Name | | | |
| 4\$* Groups | + New Departme | Create Department | | | |
| Teams | Department Name | | | | |
| Emergency Contacts | Department A | | | | |
| 🚓 Departments | | | | | |
| E Companies | | | | | |
| -B Import | | | | | |
| A Notifications | | | | | |
| Lo Administrators | | | | | |
| STATISTICS > | | | | | |
| SYSTEM > | | | | | |



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.

| O Dencrypt Control Center | | | | 9 Admin-demo 🕶 |
|---------------------------|-----------------|-------------------|---|----------------|
| 😤 Home | | Edit Department | | |
| ADMINISTRATION - | | Name | ÷ | |
| Lusers | | | | |
| 🖀 Groups | + New Departme | Delete Department | | |
| Teams | Department Name | E Gave | | |
| Emergency Contacts | Department A | | | |
| 🕂 Departments | Department B | | | |
| Companies | | | | |
| -🗗 Import | | | | |
| A Notifications | | | | |
| Lo Administrators | | | | |
| STATISTICS > | | | | |
| SYSTEM • | | | | |



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 \rightarrow Companies.

| O Dencrypt Control Center | | |
|---------------------------|-------------------------|--------------------------|
| A Home | | |
| ADMINISTRATION - | + New Company | |
| Lusers | Company Name | System |
| 🖀 Groups | ECHO_Connex_MSG_Bridge | Local |
| III Teams | My Company | Local |
| S Emergency Contacts | BRAVO_Connex_MSG_Bridge | bravo.dss.dencrypt.local |
| Departments | | |
| II Companies | | |
| - Import | | |
| A Notifications | | |
| Lo Administrators | | |
| STATISTICS • | | |
| SYSTEM • | | |



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.

| O Dencrypt Control Cer | nter | | O Admin-demo - |
|------------------------|------------------|---------------------------------|----------------|
| A Home | | + New Company | |
| ADMINISTRATION - | + New Company | Name | |
| 🚨 Users | Company Name | A Company Name | |
| 🛎 Groups | ECHO_Connex_MSG_ | Create Company | |
| Teams | My Company | | |
| Emergency Contacts | BRAVO_Connex_MSG | Bridge bravo.dss.dencrypt.local | |
| A Departments | | | |
| Companies | | | |
| -B Import | | | |
| A Notifications | | | |
| Lo Administrators | | | |
| | | | |
| SYSTEM • | | | |

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:

NameNew name of the companyLogoImage file to display as default avatar

Outputs:

• Modified or deleted company.

| Dencrypt Control Center | | | e Admin-demo 🕶 |
|-------------------------|----------------|---------------------------|----------------|
| A Home | | × | |
| ADMINISTRATION - | | Publish to other systems: | |
| Lusers | A My Company | bravo.dss.dencrypt.local | |
| 🚢 Groups | Logo | | |
| Teams | | | |
| S Emergency Contacts | | | |
| 2 Departments | P New Image | | |
| 🛚 Companies | Delete Company | R Save | |
| -🚨 Import | | | |
| A Notifications | | | |
| Lo Administrators | | | |
| STATISTICS . | | | |
| SYSTEM • | | | |

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 \rightarrow 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.

| O Dencrypt Control Cente | er | | Admin-demo |
|--------------------------|---|------------------------------------|---------------------------------------|
| 🖨 Home | Step 1: Upload File | Step 2: Review Changes | Step 3: Imported |
| ADMINISTRATION - | \bigtriangleup | | |
| Lusers | | | |
| 🛎 Groups | Select an excel file for upload. | Review the changes before they are | New users, groups and departments are |
| Teams | Download Template 🕹 | intended. | aquea. |
| Emergency Contacts | | | |
| - Departments | | × Cancel ✓ Confirm | |
| Companies | | | |
| import | | 📀 Valid file | |
| A Notifications | | Review changes and confirm. | |
| Administrators | 🔢 Company: My Company | | |
| TATISTICS • | 品 New Departments: | | |
| YSTEM 🕨 | Canteen Corner office 1st floor | | |
| | 뽄 New Groups: | | |
| | Group6 Group9 Group2 Group10 Group5 | | |
| | 은 New Users: | | |
| | | | |

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 \rightarrow Administrators.



| Dencrypt Control Cen | iter | | | | e Admin-demo |
|----------------------|----------------|----------------|----------|------------------------|--------------|
| 쑭 Home | | | | | |
| ADMINISTRATION - | Administrators | | | | |
| Lusers | + New - Delete | | | | |
| 🛎 Groups | Username | Role | Companie | S | |
| Teams | dencrypt-admin | Service Access | \$ All | Lock Reset Password | |
| Emergency Contacts | iel | Service Access | \$ All | Lock Reset Password | |
| Companies | Admin-demo | Service Access | ¢ All | | |
| 🖞 Import | dencrypt-jc | Service Access | \$ All | Lock Reset Password | |
| Notifications | | | | | |
| • Administrators | | | | | |
| | Permissions | | | | |



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 ad- ministrator at the first login. |
| Role | Specify the administrator role [Roles and Permissions 2.13]. |

Outputs:

• Administrator account created with login credentials.

| O Dencrypt Control Center | | | | × | | 🕒 Admin-demo 👻 |
|---------------------------|-----------|--------------------|--------------------|----|-----------|------------------------|
| A Home | Administr | + New | Administrator | | | |
| ADMINISTRATION - | | Username | Username | | | |
| Lusers | + New | Password | | | | |
| 📇 Groups | Userna | | | | Companies | |
| Teams | dencryp | Repeat Password | | - | All | Lock Reset Password |
| Emergency Contacts | iel | Role | User Admin | ÷ | All | Lock |
| A Departments | | | Create Administrat | or | | |
| Companies | Admin-c | _ | | + | All | |
| - ⁴ Import | dencrypt | -jc | Service Access | \$ | All | Lock Reset Password |

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.

| O Dencrypt Control Cente | r | | | e Admin-demo 🕶 |
|--------------------------|--------------------|-----------------------|----------|------------------------|
| A Home | Administr — Delete | Administrators | | |
| ADMINISTRATION - | dencrypt-a | dmin | | |
| Lusers | + New iel | | | |
| 📽 Groups | Usernal Admin-den | no | Companie | es |
| 📅 Teams | dencryp | Delete Administrators | All | Lock Reset Password |
| Emergency Contacts | iel | | All | Lock Reset Password |
| The Departments | Admin-demo | Senice Access | All | |
| Companies | | Connec Access | | |
| -🖞 Import | dencrypt-jc | Service Access | ¢ All | Lock Reset Password |
| A Notifications | | | | |
| Lo Administrators | | | | |

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.



| A Home | | | | |
|--------------------|----------------|----------------------------------|--------|------------------------|
| DMINISTRATION - | Administrators | | | |
| Users | + New - Delete | | | |
| Sroups | Username | Role | Compan | ies |
| Teams | dencrypt-admin | ✓ Service Access System Admin | All | Lock Reset Password |
| Emergency Contacts | iel | Company Admin User Admin | ¢ Ali | Lock Reset Password |
| Departments | Admin-demo | Santian Annan | All | |
| Companies | | Service Access | Y | |
| Import | dencrypt-jc | Service Access | \$ All | Lock Reset Password |
| Notifications | | | | |



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.

| O Dencrypt Control Center | | , i | | | ⊖ Dencrypt-ag + |
|---------------------------|----------------------|-------------------------------|-----------|------------------------|-----------------|
| A Home | Administratore | Companies: | | | |
| ADMINISTRATION - | Partiti au autra | Demo | | | |
| Lusers | + New - Delete | Dencrypt (DEMO) | | | |
| 🖴 Groups | Username | 🛞 Finns super firma med æøå 🖽 | Companies | | |
| III Teams | dencrypt-admin | Firma X | , All | Lock Reset Password | |
| Emergency Contacts | dencrypt-fdp | Service Access | , All | Lock | |
| + Departments | | | | | |
| Companies | dencrypt-ag | Service Access | , All | | |
| -ā import | dencrypt-henrik | Service Access | All | Lock Reset Password | |
| 20 Administrators | dencrypt_jacob | Service Access | All | Lock | |
| STATISTICS . | | | | | |
| SYSTEM > | dencrypt-christoffer | User Admin | 2 - Edit | Lock Reset Password | |
| | dencrypt-jens | Service Access | , All | Lock Decet Decouver | |

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.

| O Dencrypt Control Center | | | | | O Admin-demo 🕶 |
|---------------------------|----------------|-------------------|-----------|------------------------|----------------|
| 쑭 Home | | | | | |
| ADMINISTRATION - | Administrators | | | | |
| 🚨 Users | + New - Delete | | | | |
| 뾻 Groups | Username | Role | Companies | | |
| III Teams | dencrypt-admin | Service Access | All | Lock Reset Password | |
| Emergency Contacts | iel | Service Access \$ | All | Lock Reset Password | |
| 📇 Departments | Admin dama | | A.I. | | |
| I Companies | Admin-demo | Service Access | | | |
| -🔁 Import | dencrypt-jc | Service Access \$ | All | Lock Reset Password | |
| A Notifications | | | | | |
| Lo Administrators | | | | | |
| STATISTICS . | Permissions | | | | |

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 \rightarrow 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. <i>All companies</i> 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. |

• 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 \rightarrow 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 compa- |
| | nies 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. |

• 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 \rightarrow 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 if users with status: Registered, Invited, Revoked, Created.



| O Dencrypt Control (| Center | | | Θ Α |
|-------------------------|-----------|------------------------|---|-------------------------|
| 😤 Home | Conney | | | |
| ADMINISTRATION • | Connex | Table | | |
| STATISTICS - | _ Show As | Registered | Invited | Peunkari Createri |
| J Calls | 12 | Tiogiatariou | initia | oreated |
| Ressages | 10- | | | |
| Ser Statistics | | | | |
| SYSTEM • | 8- | | | |
| | 6 | | | |
| | | | | |
| | 4- | | | |
| | 2- | | | |
| | | | | |
| | 0 | ECHO_Connex_MSG_Bridge | My Company | BRAVO_Connex_MSG_Bridge |



7.15.2 Download user statistics

Download user statistics as .csv

| Step 1: O | pen Statistics \rightarrow | 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 re- |
| | vocation |

Outputs:

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



| Companies | Data | Format |
|-------------------------|----------------|-------------------|
| ECHO_Connex_MSG_Bridge | UserID | Download as CSV 🛃 |
| My Company | Name | |
| BRAVO_Connex_MSG_Bridge | Email | |
| | Phone number | |
| | Company | |
| | Department | |
| | Title | |
| | Created | |
| | Calls | |
| | Messages | |
| | Connex | |
| | Status | |
| | Last Connected | |
| | Last Invited | |
| | 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 \rightarrow 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 \rightarrow 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)

| ^ | | | | | | |
|-------------------------|----------------------|--|-------------------------|-------|---------------|--------|
| Dencrypt Control Center | | | | | Admin- | demo 🔻 |
| 😤 Home | Licenses | | | | | |
| ADMINISTRATION ► | LICCHSCS | | Domoining licenses | | | |
| STATISTICS > | | | Remaining licenses | | | |
| SYSTEM - | | | | | | |
| M Browser Verification | | - | Remaining Remaining | Jsed | | |
| Password Policies | | | | | | |
| Licenses | Remaining Expires | 88 2022-07-01 | | | | |
| Custom Attributes | Total Licenses | 100 | | | | |
| Standard Messages | | Serial: 83b08066-cdea-4fc8-be7e-584 Upload License File | 579f13067 | | | |
| 🖹 Logs | | | | | | |
| Certificates | Companies | | | | | |
| Apps | | | Jsers created by compan | ies | | |
| Servers | | | | | | |
| ${\mathscr O}$ Bridges | | | | | | |
| E Features | Company | | | Users | Maximum Users | |
| Alerts | ECHO_Connex_M | SG_Bridge | | 1 | Not Set | |
| 6 Backup | My Company | | | 11 | Not 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.

| SYSTEM - | | × | |
|----------------------|---|------------------|---------------|
| Browser Verification | Restrict Licenses | Lined | |
| Password Policies | Company: My Company | Used | |
| Licenses | Enter the number of maximum users the company can create. | 1e | |
| E Custom Attributes | Total Leave empty to unset. | | |
| Standard Messages | D Onlimited | 79/13067 | |
| 🖺 Logs | | ve | |
| Certificates | Companies | | |
| E Apps | Users crea | ted by companies | |
| Servers | | | |
| & Bridges | | | |
| E Features | Company | Users | Maximum Users |
| Alerts | ECHO Conney MSG Bridge | 1 | Not Set |
| C Backup | My Company | 11 | Not Set |
| 6 Maintenance | wy company. | | NUCUL |

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 \rightarrow 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.

| O Dencrypt Control Cente | r | | | | | | ⊖ Admin - |
|--------------------------|------------|----------------------|---------------------|--------------------------------------|---------|---|--------------------------------|
| 😤 Home | | | | | | | |
| ADMINISTRATION > | Apps | | | | | | |
| STATISTICS . | | | | | | | |
| SYSTEM - | Download C | op Variai Current | nts File | | | | |
| M Browser Verification | | Group | | | | | |
| Password Policies | Group | Icon | Name | Id | os | Ref | Link |
| Licenses | Connex | 0 | Dencrypt Connex | com.dencrypt.tngStore | ios | dencrypt-connect://? | https://itunes connex/id96 |
| Standard Messages | Message | \bigcirc | Dencrypt Message | com.dencrypt.messages | ios | dencrypt-messages://? | https://itunes message/id1 |
| Certificates | | | Dencrypt Message | dk.dencrypt.android.dencrypt_message | android | http://dencrypt_message.android.dencrypt.dk/provisioning/ | https://play.g id=dk.dencry |
| E Apps | Talk | 0 | Dencrypt | dk.dencrypt.dencrypt_android | android | http://www.dencrypt.dk/provisioning/ | https://play.g |
| Servers | | $\mathbf{\nabla}$ | Talk | | | | id=dk.dencry |
| ∂ Bridges | 4 | | | | | | • |
| E Features | | | | | | | |
| Alerts | | | | | | | |
| A Backup | | | | | | | |





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 \rightarrow 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 \rightarrow Custom Attributes.

| O Dencrypt Control Center | | |
|---|---------------------------------------|-----------------------------|
| ADMINISTRATION > | Custom Attrik | outes ^{Yrs.} |
| SYSTEM - | + New Attribute | Used By |
| Browser Verification Password Policies | Employee Number | All |
| Licenses | Custom Attribute Favorite Magazine | Another Company, My Company |
| Standard Messages | | |
| Logs Certificates | | |
| Servers | | |

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.

| O Dencrypt Contro | l Center | v) | O Admin-demo - |
|----------------------|------------------|------------------------|----------------|
| A Home | Attribute | <u>^</u> | |
| ADMINISTRATION > | Name | Available For: | |
| STATISTICS > | A Attribute Name | All Companies | |
| | | Selected Companies | |
| SYSTEM - | | Selected Companies: | |
| Browser Verification | | ECHO_Connex_MSG_Bridge | |
| Password Policies | | My Company | |
| Licenses | | + Add | |
| E Custom Attributes | | | |
| Standard Messages | | | |

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.



| ADMINISTRATION → Customize attributes for user STATISTICS → SYSTEM → Password Policies Custom Attribute Password Policies Custom Attribute Custom Attribute | 🖀 Home | Custom Attrib | Attribute | |
|--|----------------------|-------------------------------|------------------|---------------------|
| STATISTICS > SYSTEM + | ADMINISTRATION • | Customize attributes for user | Name | Used By: |
| VSTEM | TATISTICS | | A My Attribute | All Companies |
| Browser Verification Browser Verification Password Policies Licenses Favorite Magazine Custom Attribute Cose Favorite Magazine Cose | SYSTEM - | + New Attribute | | Selected Companies |
| Qie Provensive Vermication Employee Number Plassword Policies Custom Attribute Bi Lienness Custom Attribute Bi Costom Attributes Colose Construint | | Name | | Selected Companies: |
| A Password Policies Custom Attribute Custom Attribute Favorite Magazine Standard Messages | Browser Verification | Employee Number | | My Company |
| Licenses Custom Attribute Costom Attributes Costom Attributes | Password Policies | Employee Humber | | Test Company |
| E Custom Attributes | Licenses | Custom Attribute | Delete Attribute | |
| Stundard Messages | Custom Attributes | Favorite Magazine | | Close Save |
| S Standard Messages | a custom Attributes | _ | | |
| | Standard Messages | | | |
| Logs | 🖥 Logs | | | |
| Certificates | Certificates | | | |
| | Servers | | | |



7.20.3 Set User Attribute

Set the value of a custom attribute for a user

Step 1: Open Administration \rightarrow 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 \rightarrow 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 \rightarrow 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],

| O Dencrypt Control Center | | | | | | O Admin-dem |
|---------------------------|---------|-------------------|--|---------|----------------------|------------------|
| A Home | 💎 Filte | ər | | | | + Download |
| DMINISTRATION ► | | | | | | |
| TATISTICS > | | | 1 2 3 4 5 6 7 8 9 10 11 | | | |
| STEM - | | | | | | |
| Browser Verification | | EventID | Details | Status | Username (Userid) | Time |
| Password Policies | + | STDMSG- | Standard message 'This is a long automated reply which does not hold any | SUCCESS | Admin- | 12:24 19. Mar 22 |
| Licenses | | CREATE | 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 | | demo (14) | |
| Custom Attributes | | | guess you can't have e | | | |
| Standard Messages | + | 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 |
| Logs | + | + STDMSG- | Standard message 'Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras | SUCCESS | Admin- | 12:18 19. Mar 22 |
| Certificates | | OREATE | portitor est sed, lobortis quam. Donec felis tellus, lobortis et fermentum eu, | | denio (14) | |
| Apps | | | vestibulum | | | |
| Servers | × | STDMSG- DELETE | Standard message with id '1' has been deleted | SUCCESS | Admin- demo (14) | 12:17 19. Mar 22 |
| Bridges | + | STDMSG- CREATE | Standard message 'hi' has been created | SUCCESS | Admin- demo (14) | 12:17 19. Mar 22 |
| Features | i | LOGIN- | 127.0.0.1 login as admin-demo | SUCCESS | Admin- | 12:10 19. Mar 22 |
| Alerts | | ATTEMPT | - | | demo (14) | |
| Backup | i | LOGIN- ATTEMPT | 127.0.0.1 login as admin-demo | SUCCESS | Admin- demo (14) | 17:38 13. Mar 22 |
| Maintenance | × | COMPANY- | Company id 7 has been deleted | SUCCESS | Admin- | 14:15 24. Feb 22 |
| | | DEMONIE | | | d = m = (d A) | |

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 \rightarrow 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 "O" 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. |

• Updated password policy.

| O Dencrypt Control Ce | Admin-demo 👻 |
|-----------------------|--|
| 쑭 Home | Length |
| DMINISTRATION 🕨 | Minimum amount of characters required in passwords. |
| TATISTICS • | 9 |
| YSTEM - | Max. Age (Days) Duration of the password. The administrator will automatically be prompted to change password when it is expired. Set to 0 for infinite |
| Browser Verification | password age. |
| Password Policies | 0 |
|) Licenses | Min. Age (Hours) Passwords cannot be change for often than this. |
| Custom Attributes | 0 |
| Standard Messages | Enforce Password History |
| i Logs | Determines the number of unique new passwords that will be associated with administrators before an old password can be reused. |
| Certificates | 0 |
| Apps | Login Attempts The administrator will be denied access when the login attempts are used on wrong password. The administrator can only be unlocked by |
| Servers | system admin or service access. Set to 0 for initiate login attempts. |
| Bridges | 10 |
| Features | Require Capital Letter |
| Alerts | Require Special Character |
| | Require Numeric Character |

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 \rightarrow 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. |

• 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 \rightarrow 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 | Remote system defined. Await generation of own con- |
| request missing | nection request. |
| Pending | Await connection request from the remote system. |
| Active | Bridge connection established. |
| | - |

- 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.

| Dencrypt Control Cente | r | | | | | | | e dencrypt-admin |
|------------------------|----------------------------------|-----------------------|---------------------------|------|------------------|--------------|-----------------|-------------------|
| Home | System ID | System Name | DNS | Port | Last Updated | State | | Action |
| MINISTRATION > | system1.dencrypt.test | System1 | dsb01.sys1.dencrypt.local | 443 | Not available | Connection F | tequest Missing | 0 - |
| ATISTICS | | | | | | | | 8.4 |
| STEM - | system2.dencrypt.test | System2 | dsb01.sys2.dencrypt.local | 443 | Not available | Pending | | . • |
| Browser Verification | system3.dencrypt.test | System3 | dsb01.sys3.dencrypt.local | 443 | 2019-02-24 10:20 | Pending | | |
| Password Policies | system4.dencrypt.test | System4 | dsb01.sys4.dencrypt.local | 443 | 2020-08-31 16:13 | Active | | . • |
| Licenses | | | | | | | Connection | |
| Standard Messages | Your System | | | | | | + Sync Data | (Remote to Local) |
| Logs | Surtan ID: local des dans unt dk | | | | | | → Sync Data | (Local to Remote) |
| Contificator | System Name: Local Development | | | | | | Check Co | nnection |
| Germidates | Port: 443 | pt.dk | | | | | | |
| Servers | Change these settings you | r DSB's configuration | | | | | | |
| Bridges | | | | | | | | |
| Features | | | | | | | | |
| Verts | | | | | | | | |
| Backup | | | | | | | | |
| | | | | | | | | |



7.25 Certificates

7.25.1 Servers

Display server certificates

| Step I: Open System \rightarrow Certificates. | Step 1: | Open System \rightarrow 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.



| O Dencrypt Control Center | | | | 9 Admin-demo • |
|---------------------------|--------------------------|----------------------|--------------------|------------------------|
| 谷 Home | 🛄 Servers 🌲 Push Notific | cations Servisioning | | |
| ADMINISTRATION • | | Certificat | e Authority State: | |
| STATISTICS > | | IS | SUING | |
| SYSTEM - | | | | |
| Browser Verification | | N OK | 20 May 2027 | |
| Password Policies | <u><u> </u></u> | V UK | 20. May 2021 | · Install Certificates |
| Licenses | DCM01 | ✓ок | 20. May 2027 | Install Certificates |
| Custom Attributes | Root certificate | ✓ Valid | 20. May 2027 | |
| Standard Messages | Intermediate certificate | Near Expiration | 5. May 2022 | |
| Logs | Leaf certificate | ✓ Valid | 28. Sep 2022 | |
| Certificates | DPS01 | √ок | 20. May 2027 | Install Certificates |
| Apps | Root certificate | ✓ Valid | 20. May 2027 | |
| Servers | Intermediate certificate | Near Expiration | 5. May 2022 | |
| Ø Bridges | Leaf certificate | ✓ Valid | 5. Oct 2022 | |
| E Features | Trusted certificate | ✓ Valid | 1. Jan 2024 | |
| Alerts | S DDB01 | √ок | 6. Nov 2022 | |
| Ch. Duralizar | | | | |

Figure 76: Server certificates.

7.25.2 Push Notifications certificates

Display push certificate details.

Step 1: Open System \rightarrow Certificates.

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

Parameters:

ApplD: 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.

| O Dencrypt Control Center | | | | | | O Admin-demo 🕶 |
|---------------------------|-----------------------|-----------------|-------------|---|------------------|----------------|
| A Home | Servers A Push No | tifications 🔤 P | rovisioning | | | |
| ADMINISTRATION . | | | | | | |
| STATISTICS > | + Add Certificate | | | | | |
| SYSTEM 🔻 | AppID | Cert Type | Issuer | Capabilities | Expires | Delete |
| Browser Verification | com.dencrypt.messages | Production | Apple | apple-background | 2022-11-06 09:58 | Telete |
| Password Policies | | | | apple-voip | | |
| Licenses | com.dencrypt.messages | Development | Apple | apple-background apple-message | 2022-11-06 09:58 | Telete |
| E Custom Attributes | | | | apple-voip | | |
| Standard Messages | com.dencrypt.tngStore | Production | Apple | apple-background apple-message | 2022-11-06 09:21 | Telete |
| 🖺 Logs | | | | apple-voip | | |
| Certificates | com.dencrypt.tngStore | Development | Apple | apple-background apple-message | 2022-11-06 09:21 | Telete |
| I Apps | | | | apple-voip | | |
| Servers | | | | | | |

Figure 77: Push notification certificates.

Install push certificate.

Step 1: Open System \rightarrow 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.FileCapability: Capability the push certificate is configured for.

Certificate file provided by Dencrypt

Outputs:

• New certificate installed or removed.

| O Dencrypt Control Cer | nter | (| ~ | | ⊖ Admin-demo • |
|------------------------|-----------------------|-----------------------------|----------------|------------------|----------------|
| 🖀 Home | 💻 Servers 🌲 Push | Add Push Certificate | ^ | | |
| ADMINISTRATION > | | Select App | 0 | | |
| STATISTICS . | + Add Certificate | AppID | | | |
| SYSTEM - | AppID | | ies | Expires | Delete |
| M Browser Verification | com.dencrypt.messages | Арр Туре | ble-background | 2022-11-06 09:58 | Telete |
| Password Policies | | | ple-voip | | |
| E Licenses | com.dencrypt.messages | Issuer | ble-background | 2022-11-06 09:58 | Telete |
| Custom Attributes | | Cert Type | ple-voip | | |
| Standard Messages | com.dencrypt.tngStore | Capabilities Certificate | ble-background | 2022-11-06 09:21 | Telete |
| Logs | | As File | ble-voip | | |
| Certificates | com.dencrypt.tngStore | As Text | ble-background | 2022-11-06 09:21 | Telete |
| Apps | | + 400 | ple-voip | | |
| | | | | | |

Figure 78: Create new push notification certificate.

7.25.3 Provisioning Certificates

View existing provisioning certificates

Step 1: Open System \rightarrow 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 \rightarrow 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

| O Dencrypt Control C | Center | | | | | \varTheta Adam |
|----------------------|------------------------|---|---|-------------------------------------|--------------------------|----------------|
| A Home | 🖳 Servers 🌲 F | Push Notifications | _ | | | |
| STATISTICS . | Public Trusted | Server Certificate | | | | |
| YSTEM - | Certificate for active | ate.domain.test issued by a Public Certif | icate Authority. | | | |
| Browser Verification | | | | | | |
| Password Policies | | | | | | |
| Licenses | | Download CSR | | Upload C | Certificate | |
| Standard Messages | | request core non-the provisioning. | | of: | rifeste | |
| 🖥 Logs | _ | | _ | The Associated bundle (if provid | ICA intermediate (ed) | |
| Certificates | | | | The sequence is critic order. | al and must be in that | |
| Apps Sensorr | Client Key and | Certificate for MDM As | sisted Provisioning | | | |
| 9 Bridges | Key and Certificate | to distribute to Apps via MDM for establ | shing initial trust in provisioning proce | 35. | | |
| Features | | | | | | |
| Alerts | Status | Tag | Serial Number | Issued | Expires | Action |
| Backup | ACTIVE | Main Provisioning | 248 | Not available | Not available | . ⇒ |
| Maintenance | REVOKED | Main Provisioning | 245 | Not available | Not available | |
| | | Destruct | | Alex available | Alex available | |

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 \rightarrow Features.

Outputs:

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

| Dencrypt Control Ce | nter | 🕒 Admin-demo 🔻 |
|----------------------|---|----------------|
| A Home | | |
| DMINISTRATION . | | |
| ATISTICS > | + New Feature | |
| /STEM 🕶 | ID FEF35A81-46A3-4AA2-A9BE-5CCEE7D4E689 | |
| Browser Verification | Name Enable Messages in Connex | |
| Password Policies | Version 1 | |
| Licenses | Remove Feature | |
| Custom Attributes | | Enabled |
| Standard Messages | D B262E12C-7EE0-4183-A0E9-EC34CBE6A751 | |
| à Logs | Name Allow Connect to use external shate and videos | |
| Certificates | | |
| Apps | Version 1 | |
| Servers | Heiliove reature | Disabled |
| P Bridges | Synchronize Global Settings | |
| Features | <dencrypt_settings></dencrypt_settings> | |
| Alerts | <reatures> <feature></feature></reatures> | |
| | <version>1</version> | |

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



Outputs:

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

| Dencrypt Control Ce | nter | | Admin-demo |
|----------------------|--|---|--|
| ¥ Home | | | |
| DMINISTRATION . | SMTP Credentials | Notifications | System Report |
| TATISTICS • | Insert credentials for sending mail from the DCC. | Send a notification when an important event occurs. | Send a monthly report containing following information about the system: |
| /STEM 👻 | Host | Note: STMP Credentials must be configured. Leave email empty to disable. | Amount of users and registered user by company Configuration dependence |
| Browser Verification | | Email | Gerunicate expiration times |
| Password Policles | Protocol | | Leave email empty to disable. |
| Licenses | Port | Notify on server errors Notify on certificate renewal errors | Email |
| Custom Attributes | O 465 🗘 | Notify on certificate renewal | Send Benort B Save |
| Standard Messages | Username | Send Notification | Please save before sending report |
|) Logs | 8 | Please save before sending notification | |
| Certificates | Password | | |
| Apps | Crant Cran | | |
| E Servers | Send From | | |
| P Bridges | Save | | |
| Features | | I | |
| Alerts | | | |
| Backup | | | |

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.

| То | run | а | bac | kup |
|----|-----|---|-----|-----|
|----|-----|---|-----|-----|

| Step 1: Open System \rightarrow Backup. |
|---|
| Step 2: Select destination by checking <i>Remote</i> or <i>local</i> . |
| Step 3: Tap <i>Backup now</i> |
| Parameters:RemoteBackup destination is a remote server.LocalDownload a backup to the local server |
| Outputs: Encrypted backup stored on a remote and/or a local machine. |

Configure backup

Step 1: Open System \rightarrow 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.

| Dencrypt Control Cente | Я. | Admin-c | iemo |
|------------------------|---|---|------|
| Home | Keypair | Remote Backup | |
| MINISTRATION • | Generate a public/private keypair on the surface to use for approximation and | | |
| ATISTICS ► | signing of your backup file. Download the keypair of use for encryption and signing of your backup file. Download the keypair and store it safely outside the system. | Disabled Enabled | |
| STEM 🔻 | | Destination | |
| Browser Verification | Status: Generated 5. May 2021 P Generate & Download | Secure Copy (SCP) [Linux Only] | |
| Password Policies | | Connection | |
| Licenses | Backup Content | user @ host -P port | |
| Custom Attributes | Backup includes server configuration, logs, user data, phonebook configuration, server certificates, client certificates, intermediate certificates, all keys incl. | Password | |
| Standard Messages | private keys, message attachments and registration status. Content is always encrypted and signed before leaving the environment. Click here to see the full | Password | |
| Logs | list of backed up content. | Remote Folder | |
| Certificates | Bun | /fullpath/to/directory | |
| Apps | Start an encrypted backup to the configured remote server and/or download it | Filename | |
| Servers | locally to your browser. | Name of your backup file unloaded to remote service | |
| Bridges | Remote (Last run: No backup) Local | backup | .zip |
| Features Alerts | Backup Now | Do you want append date to your backup file to prevent overwriting previo backups? | us |
| Backup | | Append Date (e.g. backup2018-12-18T22:40:45+02:00.zip) | |
| Maintenance | | Schedule & Notification | |
| | | Time: 02:00 \$ | |
| | | Weekday: All | |
| | | Day on the Month: All \$ | |
| | | Month: Every \$ | |
| | | You need to configure email to send notifications | |
| | | D Sma | |

Figure 82: Manage backup

7.29 Display operational mode

Display the operational mode

Step 1: Open System \rightarrow Maintenance.

Outputs:

• List of operational modes per server component.



Public

| O Dencrypt Control Ce | enter | | 9 A |
|-----------------------|-------------|------------|------------|
| 😤 Home | Set To: | | |
| DMINISTRATION ► | Maintenance | Mode | |
| TATISTICS • | | lode | |
| YSTEM 🕶 | Server | Mode | |
| Browser Verification | DCC | Production | |
| Password Policies | DCM01 | Production | |
| Licenses | DPS01 | Production | |
| Custom Attributes | DDB01 | Production | |
| Standard Messages | DCS01 | Production | |
| Logs | DCS02 | Production | |
| Certificates | DMS01 | Production | |
| Apps | | | |
| Servers | | | |
| Bridges | | | |
| Features | | | |
| Alerts | | | |
| Backup | | | |

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":

| 🔓 Change Password |
|-------------------|
| 🔎 API Key |
| C→ Logout |

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

| O Dencrypt Control Ce | nter |
|-----------------------|--|
| A Home | |
| ADMINISTRATION ► | API Key |
| STATISTICS > | API Key for accessing Management REST API. |
| SYSTEM • | Key: |
| | ONzfDDAFkobN1fKkXixfz8gvX17wQlpF8YUMBusWTDKUTufQPM6pVnVTp2pfoPUw |
| | |

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"

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

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

Create a department called "IT Department"

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 \rightarrow 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.

| O Dencrypt Control Center | | | |
|---------------------------|---------------|------------|--|
| A Home | Set To: | | |
| ADMINISTRATION ► | Maintenance I | Mode | |
| STATISTICS > | | ode | |
| SYSTEM 🔻 | Server | Mode | |
| 🖓 Browser Verification | DCC | Production | |
| Password Policies | DCM01 | Production | |
| Licenses | DPS01 | Production | |
| E Custom Attributes | DDB01 | Production | |
| Standard Messages | DCS01 | Production | |
| Logs | DCS02 | Production | |
| Certificates | DMS01 | Production | |
| Apps | | | |
| Servers | | | |
| & Bridges | | | |
| Features | | | |
| Alerts | | | |
| A Backup | | | |

Figure 84: Toggle operational mode.



A.1.1 Configuration Change

| Step 2: Tap <i>Save</i> . | |
|---|---|
| Outputs: DCM server reconfigured. | |
| Parameters: | |
| Common Fields | |
| rabbit_mq/server_ip | IP address of the RabbitMQ server. Not edible. |
| common/name | Internal name of the server. |
| common/hostname | The hostname part of the fully qualified domain name (FQDN). <i>Not edible.</i> |
| common/hostname | The hostname part of the fully qualified domain name (FQDN). <i>Not edible.</i> |
| common/system_domain | DNS of the system domain. |
| common/external_ip | External IP for servers with the external interface. |
| common/dns | DNS entry. |
| common/server_type | Internal server abbreviation of the server type. Not edi- ble. |
| common/network_type | Whether network type is configured as NAT or DirectIP. |
| HAProxy//name | Internal technical name of the interface. |
| HAProxy//frontend | Address to receive traffic from. |
| HAProxy//backend | Address to send traffic to. |
| HAProxy//verify | Whether to verify client certificate in TLS |
| HAProxy//curve | Curve to accept |
| HAProxy//server | Type of server to be specified in the HAproxy configura- tion file |
| HAProxy//crl | Whether to reject connections in the certificate revoke list |
| HAProxy//certificate | Which certificate on the server to use |
| certificates/common_name | Common name used in the HTTPS certificates. |

A.2 Dencrypt Control Center: Configuration Parameters:

DCC Configuration

HAProxy/WebSSL/.. Web interface for administrators.

A.3 Dencrypt Certificate Manager: Configuration

Parameters: DCM Configuration

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

Configuration Change

Step 1: Fill in the fields.



A.4 Dencrypt Provisioning Server: Configuration Parameters:

DPS Configuration

| ddb_internal_ip | Internal IP of the DDB. |
|-------------------------------------|--|
| dcm_internal_ip | Internal IP of the DCM. |
| invitation_expiry_time | Amount of hours until the invitation is expired. |
| invite_version | Internal version of invitation. Not edible. |
| permanent_invited_userids | Space separated list of user IDs that can reuse invites |
| | AND never expires. |
| reusable_invited_userids | Space separated list of user IDs that can reuse invites. |
| enable_legacy_provisioning | Enable Dencrypt Talk provisioning. |
| https_invite/enabled | Whether to use unified HTTPS links for provisioning. |
| mail_conf/mail_enabled | Whether you should allow provisioning through email. |
| mail_conf/mail_server | Address of the mail server to use for email provisioning. |
| mail_conf/mail_port | Port of the mail server to use for email provisioning. |
| mail_conf/mail_protocol | Protocol of the mail server to use for email provisioning. |
| mail_conf/username | Username of the mail server to use for email provision- |
| mail conf/nassword | Password of the mail server to use for email provision- |
| | ing. |
| mail conf/mail send from | Which email invites are seen as being sent from. If |
| | empty, it uses the username specified above. |
| mail conf/mail voipaen1 subiect | Text of the email subject for VoipGen1. |
| mail_conf/mail_voipgen1_name | Name of the VoipGen1 application as presented in the |
| | email. |
| mail_conf/mail_messagegen1_subject | Text of the email subject for MessageGen1. |
| mail_conf/mail_messagegen1_name | Name of the MessageGen1 application as presented in |
| | the email. |
| mail_conf/mail_multicomgen1_subject | Text of the email subject for MultiComGen1. |
| mail_conf/mail_multicomgen1_name | Name of the MultiComGen1 application as presented in |
| | the email. |
| mail_conf/logo | Name of the logo file on local server /usr/local/dencryp- |
| | t/dcs/emails/*. |
| maii_conj/logo_alt_text | ing the logo. |
| mail conf/customer | Name of the customer presented in the invitation. |
| mail conf/supportEmail | Support email presented in the invitation. |
| mail conf/supportPhone | Support phone number presented in the invitation. |
| mail conf/retry delay | Number of seconds to wait before retrying to send the |
| - ,. ,- , | email. |
| sms_conf/sms_enabled | Whether you should allow provisioning through SMS. |
| sms_conf/method | GET or POST request method to SMS provider. |
| sms_conf/url | Full URL to SMS service. Use receiver, message and |
| | sender as variables, encapsulated with curly brackets. |
| sms_conf/body | Raw body of POST request. Ignored for GET requests. |
| | Use receiver, message and sender as variables, encapsu- |
| | lated with curly brackets. |
| sms_conf/headers | List of HTTP headers, separated by semicolon. Use re- |
| | ceiver, message and sender as variables, encapsulated |
| | with curly brackets. |
| sms_conf/talk_text | Prepended text in the SMS for VoipGen1. |
| sms_conf/messages_text | Prepended text in the SMS for MessageGen1. |
| sms_conf/dencrypt_text | Prepended text in the SMS for MultiComGen1. |
| sms_conf/sender | Subject of the SMS sender. |
| certificates/provisioning | Lommon name used for provisioning. |
| HAProxy/ExternalHTTPS/ | Lient interface for provisioning when accepting invita- |
| | tions. |
| HAPTOXY/INTERNAIHTTPS/ | internal server interface for Web API requests. |

A.5 Dencrypt Database: Configuration Parameters:

DDB Configuration

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



Dencrypt Communication Server: Configuration Parameters: **DCS Configuration A.6**

| DLS Configuration | | | | |
|---|---|--|--|--|
| srvrec_name | DNS of the subdomain for server records. | | | |
| db_password | Password for database connection. | | | |
| ddb_ip | Internal IP of the DDB. | | | |
| authorization | Whether to authorize user ID and password for WebAPI. | | | |
| allow_meta_data_in_push | Allow metadata such as name, SIP address etc. in push notifications. | | | |
| push encryption | Encrypt content of push notifications. | | | |
| call nush ttl | Time to live in seconds for call nush notifications. | | | |
| dh conf/dh | Natabase name to connect to | | | |
| db_conf/user | Database light to connect with | | | |
| db_conf/nascword | Database user to connect with Not adible | | | |
| db_conf/in | Database passion to connect with. <i>Not eutore.</i> | | | |
| ub_conj/ip db_conf(cont | Database IP to connect to. | | | |
| ab_conf/port | Database port to connect to. | | | |
| ddb_connection/ip | The IP of the DDB. | | | |
| ddb_connection/port | The port to connect to the DDB. | | | |
| flexisip/proxy_enabled | Whether to enable Flexisip Proxy server. | | | |
| flexisip/conference_enabled | Whether to enable Flexisip Conference server. | | | |
| flexisip/presence_enabled | Whether to enable Flexisip Presence server. | | | |
| flexisip/log_level | Verbosity of logs to output. | | | |
| flexisip/conference_factory | Uri where the client must ask to create | | | |
| | a conference. Example: sip:conference- factory@dcs.charlie.dss.dencrynt.local. | | | |
| flexisin/conference outhound proxv | Example: sin:10.10.20.184:5070:transnort=tcn. | | | |
| flexisip/sip_port | SIP port to listen on (DEPRECATED - use transports in- stead) | | | |
| flexisin/transnorts | Transports parameter of Elevisin defin- | | | |
| | ing interfaces to listen on Example. | | | |
| | sips:dcs01.mysystem.example.com:5061;maddr=192.168 | | | |
| flexisip/auth_domains | Space seperated. | | | |
| flexisip/nodes | Space separated. | | | |
| flexisip/trusted_hosts | Space seperated. | | | |
| flexisip/aliases | Space separated. | | | |
| flexisip/reg_domains | Space separated. | | | |
| flexisip/webapi | The address for the WebAPI phonebook and settings download | | | |
| flexisin/redis server | Redis address | | | |
| flexisin/redis_server | Redis nort | | | |
| flevisin/enable call loas | Whether to enable call logs | | | |
| flexisip/enuble_cuil_logs | lower limit for LIDD ports used for modia relay | | | |
| flexisip/uup_inin_port | Lower limit for UDP ports used for media relay. | | | |
| Jiexisip/uup_mux_port | Opper limit for ODP ports used for media relay. | | | |
| flexisip/force_public_lp_for_sap_masqueraaing | Force public IP in SUP (needed when Flexisip is benind | | | |
| | NAT and HAProxy). | | | |
| flexisip/devices_per_user | Number of devices allowed per user. | | | |
| lime/curve_id | Curve to use, shall be either Curveld::CURVE25519 or | | | |
| | Curveld::CURVE448. | | | |
| lime/persistent_connections | Whether to persist connection. | | | |
| lime/lime_db_host | Lime database host. | | | |
| lime/lime_db_name | Lime specific database name to connect with. | | | |
| lime/log_level | Log level of Lime. Disabled is recommended. | | | |
| lime/db_logs_enabled | Whether database logs are enabled. | | | |
| lime/auth realm | Typically same as system domain. | | | |
| lime/auth nonce key | Random string(12 characters minimum length) specific | | | |
| · , | to each server and is private. Leave empty to autogener- | | | |
| lime/min nonce validity neviad | ale a 20-chialacter 1011g Stillig. The suther tigstion is simed to provide some time usage | | | |
| iirrie/min_nonce_vallaity_period | i rie autrientication is almed to provide a one-time usage | | | |
| | nonce, it is not strictly enforced by storing valid once, in- | | | |
| | stead we use a short living period, the maximum validity | | | |
| ruary 2023 Pu | blperiod will be twice the minimum one, paluesis in sec- | | | |
| certificates (service records | Common name used for SIDS certificator | | | |
| nublic interfaces (uchani nort | Common name used for SIFS Leftifildles. | | | |
| puonic_initerjutes/webupi_port | Fort to public WebAPI. | | | |

A.7 Dencrypt System Bridge: Configuration

| Parameters: | |
|-------------------|--|
| DSB Configuration | |

| internal_port | Internal port used for bridge interface. |
|-----------------------|--|
| external_port | External port used between bridges. |
| haproxy_bridge_config | 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 \rightarrow 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.

| O Dencrypt Control Center | | | | | | | e dencrypt-admin |
|---------------------------|--|-------------|---------------------------|------|------------------|---------------------------|------------------|
| 备 Home | System ID | System Name | DNS | Port | Last Updated | State | Action |
| ADMINISTRATION > | system1.dencrypt.local | System1 | dsb01.sys1.dencrypt.local | 443 | Not available | Connection Request Missin | 9 8 - |
| STATISTICS . | | | | | | | |
| SYSTEM - | system2.dencrypt.local | System2 | dsb01.sys2.dencrypt.local | 443 | Not available | Pending | ۰ * |
| Browser Verification | system3.dencrypt.local | System3 | dsb01.sys3.dencrypt.local | 443 | 2019-02-24 10:20 | Pending | ۰ چ |
| Password Policies | system4.dencrypt.local | System4 | dsb01.sys4.dencrypt.local | 443 | 2020-08-28 09:44 | Active | ۰ چ |
| E Licenses | | | | | | | |
| Standard Messages | Remote System ID | | | | | | + New |
| Logs | Your System | | | | | | |
| Certificates | Custom ID: local des desenset die | | | | | | |
| Servers | System ID: local dss.dencrypt.dk System Name: Local Development DNS: local.dsb.dss.dencrypt.dk | | | | | | |
| 🔗 Bridges | Port: 443 Change these settings your DSP's cor | afiguration | | | | | |
| Features | charge areae acturgs your DOD's con | ngurason | | | | | |
| Alerts | | | | | | | |
| 🗛 Backup | | | | | | | |
| Maintenance | | | | | | | |

Figure 85: Remote systems.

Establish a trusted connection.

Step 1: Open System \rightarrow Bridges.

- Step 2: Select the remote system and tap Actions.
- 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:

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

Outputs:

• Remote connection established.

| Home | | | | | Last | | |
|----------------------|--|--------------------------|--------------------------------|------|----------------------|-----------------------|---------------|
| MINISTRATION . | System ID | System Name | DNS | Port | Updated | State | Action |
| (TISTICS) | bravo.dss.dencrypt.local | bravo.dss.dencrypt.local | dsb01.bravo.dss.dencrypt.local | 443 | 2021-05- 25 15:27 | Active | ۰ چ |
| STEM 🔻 | delta.dss.dencrypt.local | | | | Not available | Connection Request | * |
| Browser Verification | | | | | dramabio | Connection | |
| Password Policies | | | | | | ⊢ Sync Data (Rem | ote to Local) |
| | Remote System ID | | | | | → Sync Data (Loca | I to Remote) |
| Licenses | | | | | | Check Connecti | on |
| Custom Attributes | Your System | | | | 0 | Configuration | |
| Standard Massages | | | | | | Import Connecti | on Request |
| otanuaru messages | System ID: echo.dss.den | rypt.local | | | | Export Connecti | on Request |
| Logs | DNS: dsb01.echo.dss.der | crypt.local | | | | Delete | |
| Certificates | Port: 443 Change these settings you | r DSB's configuration | | | | | |
| Apps | | | | | | | |
| Servers | | | | | | | |
| Bridage | | | | | | | |

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 \rightarrow 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.

Crete and modify features

Step 1: Open System \rightarrow 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 Synchonize Global Settings.

Parameters:

IDUnique feature identifier.NameDescriptive name of the feature.

Version Feature version number.

Outputs:

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

| O Dencrypt Control C | Center | Dencrypt-admin |
|----------------------|---|--|
| 骨 Home | | |
| ADMINISTRATION . | Save Features | Synchronize Global Settings |
| TITIOTICO . | + New Feature | <dencrypt_settings></dencrypt_settings> |
| TATISTICS | | (eatures) |
| SYSTEM - | ID FEF35A81-46A3-4AA2-A9BE-5CCEE7D4E689 | <pre>sversion>1</pre> |
| | | <enabled>1</enabled> |
| Browser Verification | Name Enable Messages in Connect | |
| | | <name>Enable Messages in Connect</name> |
| Password Policies | Version 1 | |
| B Linner | | <teature></teature> |
| 4 Licenses | Remove Feature | sversion/ sversion/ |
| Standard Messages | | <id>8262E12C-7FE0-4183-A0F9-FC34CBE6A751</id> |
| | | <name>Allow Connect to use external photo and videos</name> |
| Logs | | |
| | ID B262E12C-7FE0-4183-A0F9-FC34CBE6A751 | <feature></feature> |
| Certificates | | <version>1</version> |
| E Convers | Name Allow Connect to use external photo and videos | <enabled>U</enabled> |
| a ocivers | Manalan | <pre>sname>Enable biometric login in Connects/name></pre> |
| P Bridges | version | |
| | Remove Feature | <feature></feature> |
| Features | Er | abled <version>1</version> |
| | | <enabled>1</enabled> |

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

| Event ID | Description | Туре | Details |
|---------------|----------------------------------|--------|--|
| ADMIN-ADD | Admin: Add account | create | Administrator <username> created.</username> |
| ADMIN-LOCK | Admin: Lock account | delete | Admin with id <adminid> now is now locked.</adminid> |
| ADMIN-PWRESET | Admin: Reset password | update | Admin with id <adminid> has had reset pass-</adminid> |
| | | | word |
| ADMIN-REMOVE | Admin: Delete account | delete | Administrator id <adminid> deleted.</adminid> |
| ADMIN-UNLOCK | Admin: Unlock account | create | Admin with id <adminid> now is now un-</adminid> |
| | | | locked. |
| ADMIN-UPDATE | Admin: Configure account | update | Admin with id <adminid> has changed role to</adminid> |
| | | · | <newrole></newrole> |
| ADMIN-UPDATE | Admin: Lonfigure account | update | Admin with id <adminid> now has permission</adminid> |
| | Admin. Configure account | undata | to company lu < company lu > |
| ADMIN-OPDATE | | upuate | mission to company id < companyid |
| | Backup: Configuration | undate | Backup configuration undated |
| DACK-AUTO | undated | upuate | Backup configuration updated. |
| ΒΑΓΚ-DOWNLOAD | Backun: Manual backun | info | Backun downloaded. |
| BACK-GETKEY | Backup: Received keys | info | Kevpar retrieved. |
| BACK-KEYGEN | Backup: Keypair generated | create | Kevpair generated |
| BACK-REMOTE | Backup: Remote backup | info | Remote backup performed |
| BRIDGE-CREATE | Bridge: Add connection | create | Bridge connection for system < systemid> cre- |
| | | | ated. |
| 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></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 | update | Install intermediate certificate for DCM |
| | install | | <serverid></serverid> |
| CERI-RESEI | Server: Lertificate reset | update | State RESET to <state>.</state> |
| | Server: Root certificate install | update | Installed root for DLM <serverid></serverid> |
| | Server: LRL Install | update | Upload root LRL for DLM <serverid></serverid> |
| | Server: Install public LA | update | Lertificate installed for DPS |
| | | croato | Company < names created |
| | Company: Delete | doloto | Company < hame> created. |
| REMOVE | company. Delete | uciete | |
| COMPANY- | Company: Share group | delete | Groun id <grounid> is no longer connected to</grounid> |
| REMOVEGROUP | | | company id <company id=""></company> |
| COMPANY- | Company: Unshare group | create | Group id <groupid> is now connected to com-</groupid> |
| TOGROUP | | | pany id <company id=""></company> |
| COMPANY- | Company: Edit | update | Company < name> with id < companyid> has |
| UPDATE | | | been updated. |
| DEP-ADD | Department: Add | create | Department <name> created.</name> |
| DEP-DELETE | Depertment: Delete | delete | Department id <dep.id> has been deleted.</dep.id> |
| DEP-UPDATE | Department: Edit | update | Department id <dep.id> updated name to</dep.id> |
| | | | <newname></newname> |
| EMERG- | Emergency list: Add user | create | User <id> has been added to emergency list</id> |
| | | | <name></name> |
| EMERG-CREATE | Emergency list: Add | create | Emergency list <name> created.</name> |
| EMERG-DELETE | Emergency list: Delete | delete | Emergency list <name> has been deleted.</name> |
| | Emorgonov list. Domovo visav | delete | Erriergency list < name > has been deleted. |
| | Emergency list: Remove user | uelete | |
| REMOVELUNIALI | | | iist <fidffie></fidffie> |

Table 2: Audit log definitions

Continued on next page



| Table 7 | Continued | from | nroulour | n |
|-----------|-----------|------|----------|------|
| Table Z - | Continueu | jium | previous | puye |

| Event ID | Description | | |
|---------------|-------------------------------|--------|--|
| | Emergency list: Chare | rype | Emorgoneu liet <nomes avail<="" been="" has="" made="" td=""></nomes> |
| EMERU-SHARE | Emergency list: Share | create | Emergency list < name > nas been made avail- |
| FLIEDC | - | | able to company < companyid > |
| EMERU- | Emergency list: Unshare | delete | Emergency list <name> has been made un-</name> |
| | | 1. | available to Lompany <companyid></companyid> |
| EMERG-UPDATE | Emergency list: Edit | update | Emergency list <name> has changed name to</name> |
| | | | <newname></newname> |
| GROUP-ADD | Group: Add | create | Group name: <groupid> created.</groupid> |
| GROUP-REMOVE | Group: Delete | delete | Group id: <groupid> deleted.</groupid> |
| GROUP-UPDATE | Group: Update | update | Group name: <groupid> changed name to</groupid> |
| | | | <newname></newname> |
| GROUP-UPDATE | Group: Update | update | Group id <groupid> link to group id</groupid> |
| | | | <pre><groupiod> is set to <link/></groupiod></pre> |
| LOGIN-ATTEMPT | Admin login attempt | info | <ip> login as <admin.id></admin.id></ip> |
| MAINTENANCE- | Server: Toggle maintenance | update | Maintenance for server <id> set to on/off.</id> |
| SET | mode | | |
| PUSH-ADD | Push certificate: Add | create | Push certificate added. Id: <cert id=""></cert> |
| PUSH-REMOVE | Push certificate: Delete | delete | Push certificate removed Id: <cert id=""></cert> |
| SERVER- | Server: Toggle activation | update | Server: <id> activation status set to en-</id> |
| ACTIVATE | | | abled/disabled. |
| SERVER-ADD | Server: Add | create | Server created at <ip></ip> |
| SERVER-CONFIG | Server: Configuration update | update | Server: <id> configuration updated.</id> |
| SERVER-REMOVE | Server: Remove | delete | Server: <id> has been deleted</id> |
| 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</id> |
| SERVER-UPDATE | Server: Change IP-address | update | Server <id> changed IP to <ip>.</ip></id> |
| STDMSG-CREATE | Std Messages: Add | create | Standard message <msgid> has been cre-</msgid> |
| | 5 | | ated. |
| STDMSG-DELETE | Std Messages: Delete | delete | Standard message with id <msgid> has been</msgid> |
| | | | deleted. |
| STDMSG-ORDER | Std Messages: Move up | update | Standard message with id <msgid> has been</msgid> |
| | | | moved up in order. |
| STDMSG-ORDER | Std Messages: Move down | update | Standard message with id <msgid> has been</msgid> |
| | | | moved down in order. |
| STDMSG-UPDATE | Std Messages: Edit | update | Standard message with id <msgid> has been</msgid> |
| | | | undated |
| SYS-FEATURE | System: Feature configuration | undate | Feature settings undated |
| SYS- | Notifications: Undate | undate | Alert SMTP credentials undated. |
| NOTIFICATION | ····· | | |
| SYS- | Notifications: Undate | undate | Alert notification undated |
| NOTIFICATION | ····· | | · · · · · · · · · · · · · · · · · · · |
| SYS- | Notifications: Update | update | Alert system report updated |
| NOTIFICATION | | | · · · / · · · · · · · · · · · · · · · · |
| SYSTEM-INIT | System: Initialization | info | System initialized with user < username> |
| TFAM- | Teams: Add user | create | User <userid> has been added for team</userid> |
| ADDMEMBER | | cicuto | <teamid></teamid> |
| TEAM-CREATE | Teams: Add | create | Team < teamid > has been created |
| TEAM-DELETE | Teams: Delete | delete | Team <teamid> has been deleted</teamid> |
| ΤΕΔΜ- | Teams: Remove user | delete | User <userid> has been removed from team</userid> |
| | reality. Remove user | uciete | <pre><teamid></teamid></pre> |
| TEAM-SHARE | Teams: Share | undate | Team <teamid> has been shared with com-</teamid> |
| | | apuare | nany < comnanyid> |
| TEAM-UNSHARE | Teams: Unshare | undate | Team < teamid > has been unshared with com- |
| | icanis, onshare | apuate | nany < comnanyid> |
| ΤΕΔΜ-ΠΡΠΔΤΕ | Teams: Edit | undate | Team <teamid> has changed name to</teamid> |
| | icanio, cuit | upuale | icani <icania changea="" name="" nas="" td="" to<=""></icania> |
| | | | <newname></newname> |
| USER-ANN | User: Add | create | <newname> <firstname>.<lastname> with user id</lastname></firstname></newname> |
| USER-ADD | User: Add | create | <newname> <firstname>.<lastname> with user id <userid> has been created</userid></lastname></firstname></newname> |
| USER-ADD | User: Add | create | <newname> <firstname>.<lastname> with user id <userid> has been created. Invitation (email) has been sent to user with</userid></lastname></firstname></newname> |

Continued on next page



| Event ID | Description | Туре | 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></userid> |
| USER-REMOVE | User: Delete | delete | User <userid> has been deleted.</userid> |
| USER-REVOKE | User: Revoke access | delete | User <userid> has revoked access.</userid> |
| USER-SMS | User: SMS invitation | info | Invitation (sms) has been sent to user with |
| | | | user-id <userid></userid> |
| USER-UPDATE | User: Update | update | Userid <userid> has teams set to following:</userid> |
| | | | <list ids="" of="" team=""></list> |
| USER-UPDATE | User: Update | update | Userid <userid> has been removed from fol-</userid> |
| | | | lowing teams: : <list ids="" of="" team=""></list> |
| USER-UPDATE | User: Update | update | Userid <userid> set emergency lists to follow-</userid> |
| | | | ing: <list emergency="" ids="" of=""></list> |
| USER-UPDATE | User: Update | update | Userid <userid> has removed following emer-</userid> |
| | | | gency lists: : <list emergency="" ids="" of=""></list> |
| USER-UPDATE | User: Update | update | User id <userid> updated to following: <list< td=""></list<></userid> |
| | | | of metadat>. |
| USER-UPDATE | User: Update | update | Userid <userid> updated image.</userid> |
| USER-UPDATE | User: Update | update | Userid <userid> updated groups</userid> |
| | | | · |

Table 2 – Continued from previous page



C Version history

| Ver. | Author | Date | Notes |
|------|--------|------------|--|
| 1.0 | SS | 31-08-2020 | Initial version in 上下X 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. |