LANCOM Management Cloud

Security-relevant settings

02/2026

LANCOM SYSTEMS

Contents

1 LANCOM Management Cloud

This document describes the security-relevant settings of the LANCOM Management Cloud (LMC) It serves as a reference for the secure operation of the LMC.

2 Account and role concept

2.1 Concept of principals, memberships and accounts

2.1.1 Terminology

Principal

A technical representation of a person who can access LMC. A principal is identified at login by an e-mail address and has a technical reference (UUID) used for internal data processing in LMC.

Account

An entity that can be accessed by authenticated and authorized principals. An account is identified by a UUID and includes human-readable metadata.

Authority

A set of permissions (ACL), equivalent to the concept of roles.

Membership

A mapping that associates a principal with an authority for a specific account.

2.1.2 Concept of granting rights

1. As a first step, LMC-managed principals are invited by account administrators to an account and granted a specific level of authority. IdP-managed principals can sign up without a prior invitation. Both types of principals must complete a form and provide an email address, a password, a salutation, and a first and last name, although the last three may be fictional. Both types of principals must also accept the current Principal Terms of Use document.
2. On login, the principal is identified by the email address previously registered for that principal, which is unique in LMC installations.
3. Each account invitation must be accepted by the invited principal before it takes effect.
   a. It is possible to invite a principal and then remove the membership before the principal has accepted it, resulting in a principal profile without memberships. This is useless, but it is a valid state (the principal can log in but can access only the principal profile).
   b. The invitation is also time-limited and will expire, but the principal can still sign up (create their principal profile) after the invitation has expired, resulting in a similar state (no valid membership).
   c. For both LMC-managed and IdP-authenticated principals, a membership can be added later by sending another invitation to an account.
   d. For IdP-authorized principals, the corresponding access rights must be granted in the IdP (see also *Alternative authentication methods* on page 8).
4. The combination of a principal, a specific account ID, and a specific authority granted to that principal for that account results in a membership, which allows access to the account.
5. Any principal with no direct membership and no authority granted via IdP authorization has no access to any account and can only view and edit details in their principal profile section.

2.1.3 Account structure and tenant separation

In the LMC, we differentiate between three different account types:

- A Distribution, with distinct authorities and responsibilities at the distribution level (overarching customer management; multiple per LMC instance, and multiple per large partner customer possible).
- An Organization, with distinct authorities and responsibilities at the organization level (overarching customer management; multiple per LMC instance, usually one per partner customer).
- A Project, with distinct authorities for device, network, network security, license management, etc. (multiple per LMC instance, multiple per partner customer, usually one per end customer).

Data is strictly separated per account and can be accessed only if an individual principal has been granted membership to access that specific account.

Accounts are ordered hierarchically: a project must be created within an organization, and organizations are created under distributions. Some functions allow managing projects from the parent organization (e.g., administrator inheritance and device pools that can be used to assign devices to projects), which are described further below.

2.1.4 Least privilege principle for memberships

As a best practice, only the minimum rights required should be granted to a principal so the principal can perform a specific task in the application. In the LMC context, this means granting project administrator rights only with great care and using an authority with fewer rights whenever possible. The following authorities can be granted at each account level:

- Standard distribution-level authorities:
  - Distribution administrator: Allowed to manage organizations, administrators, and devices. Has unrestricted access to distribution information.
- Standard organisation-level authorities:
  - Organization administrator: Allowed to manage projects, principals, and devices. Has unrestricted access to organization information.
  - Organization viewer: Authorized to view, but not edit, organization-related information.
- Standard project authorities:
  - Project administrator: Allowed to manage the project, principals, and devices. Has unrestricted access to project information.
  - Technical administrator: Allowed to manage sites, networks, and devices. Project information is read-only, and managing principals is not allowed.
  - Project member: Authorized to manage and monitor the project's devices. Has read-only access to project information.
  - Rollout assistant: Used by the LMC Rollout Assistant App to simplify device claiming in this project. Allowed to add devices and read device information.
  - Hotspot operator: Authorized only to manage the hotspot.
  - Project viewer: Allowed only to view, but not edit, device- and project-related information.

For LMC-managed principals, a different authority can be granted in each account the principal can access. This also applies to IdP-authenticated principals.

If IdP authorization is configured and enabled for an account, a principal's authorities and resulting rights are derived from the roles assigned in the IdP (see also *IdP principal management* on page 10). This results in the same authority being granted per principal per account level—or no authority at all—but it cannot result in, for example, a principal being a project administrator in one project and a hotspot operator in a second project within the same organization. When using IdP principal management, it is recommended not to use the invitation mechanism to assign authorities to principals who are IdP-authorized for that account. Explicitly inviting users creates so-called "direct memberships," which override IdP-based access control.

2.2 Administrator inheritance

Administrator inheritance can be used to increase security and simplify management for Managed Service Providers (MSPs), who typically have an organization and use separate child projects for their customers. Instead of inviting principals to each project individually and managing them separately, administrator inheritance allows members of the organization to access child projects without being explicitly invited to each one. This simplifies access control because those principals can be managed centrally within the organization (e.g., when a principal leaves the company and should no longer have access to LMC accounts). It removes the need to create direct memberships in each project for all affected principals and thereby reduces the effort required to enforce access restrictions at the project level.

Direct memberships (created via explicit invitations) and administrator inheritance can be combined in mixed scenarios per principal and account. As a result, a single principal can be granted project access with different rights via administrator inheritance than those granted by accepting an invitation and receiving a direct membership. In such cases, rights granted via direct membership take precedence over inherited rights, which can result in a higher set of rights than intended through administrator inheritance. For this reason, we recommend using direct memberships in administrator inheritance scenarios only with great care. As a secure default, LMC administrator inheritance is disabled in organizations and must be enabled by organization administrators. When enabling LMC administrator inheritance, a project-level authority must be selected; this authority is applied to inherited principals across all projects within the organization.

IdP administrator inheritance can be enabled independently of LMC administrator inheritance at the organization level. In the context of IdP authentication, it works like LMC administrator inheritance as described above, but it is limited to principals managed via the IdP configuration for that specific organization. If IdP authorization is also enabled in LMC, authorities and resulting rights are derived from the values returned by the IdP and the group mappings configured during IdP setup (see also *Offboarding for IdP-managed principals* on page 14).

Project administrators can separately opt out of both LMC administrator inheritance and IdP administrator inheritance by enabling the corresponding setting in the project settings. Any change in inheritance status is recorded in the organization log. Both opt-out options are not available in Telekom Schwestercloud, as specified by contract.

3 Account security

3.1 Password security

3.1.1 General recommendations

For the LMC, we follow general recommendations on how to choose secure, memorable passwords and what to avoid, such as those provided by *the German Federal Office for Information Security*.

- Creativity is unlimited, but the password must be easy to remember. Helpful strategies include:
  - Using a sentence and taking only the first (or second or last) letter of each word
  - Replacing some letters with numbers or special characters
- Using an entire sentence as a password
  - Stringing together several words separated by special characters
  - Randomly choosing 5–6 words from a dictionary and separating them with spaces, which makes the password easy to remember and type, but hard to crack
- In general: the longer, the better. For a good password, length and complexity are crucial.
  - A short, complex password should be at least 8 characters long and contain four character types: uppercase and lowercase letters, numbers, and special characters.
  - A long, less complex password should be at least 25 characters long.
  - For Wi-Fi encryption methods such as WPA2 or WPA3, the password should be at least 20 characters long because offline attacks are possible.
- In principle, all available characters can be used (uppercase and lowercase letters, digits, and special characters such as spaces, ?!%+…).
- Unsuitable passwords include names of family members, pets, best friends, favorite celebrities, birth dates, and similar personal information. Passwords should also not consist of common variations, repetition, or keyboard patterns such as “asdfgh” or “1234abcd”.
- Avoid simply appending a few digits to the end of a password or placing common special characters (e.g., “$”, “!”, “?”, “#”) at the beginning or end of an otherwise simple password.
- Using a password manager is recommended to manage different passwords and protect the manager with one strong master password. This way, a principal only needs to remember one strong password while still using very strong, unique passwords everywhere.
- Language-specific characters and umlauts such as “ä, ö, ü, ß, €, ¢” should be avoided because they may not be available with non-German services and keyboards or may be encoded differently.

3.1.2 Passwords for principals

In the default configuration, LMC requires a password length of at least eight characters, including at least one number and one special character. It is strongly recommended to create a password that follows the guidelines stated above. In addition, the corresponding environment variable can be adjusted to enforce stronger passwords for principals. This is recommended for any private LMC installation. It is also considered good practice to use different passwords for each principal in each LMC instance, following the recommendations mentioned in *General recommendations* on page 7.

3.1.3 Passwords for Devices, Wireless SSIDs, VPNs

In general, it is highly recommended not to leave any remotely managed resource unprotected, i.e., to use password protection whenever possible. When doing so, follow general password security guidelines. In some cases, a project-wide password can be set for device configuration. We do not recommend choosing this option, and it should be used only if truly necessary. Using a different password for each device is much more secure. If a common password for device configuration per account cannot be avoided, it is strongly recommended to choose a highly secure password for that option.

3.2 2FA

To add an additional layer of access control and security, LMC-managed principals can enable two-factor authentication (2FA) for their principal. The additional secret is used to generate a time-based one-time password (TOTP). The shared secret used by the authenticator app to generate TOTPs is created by LMC. This shared secret can be stored either in an authenticator app on a mobile device or in a browser-based password manager extension on any computer. The second option is recommended only if the LMC principal can ensure they are the only person with access to that browser's password manager extension. Security measures to protect browser password manager extensions or mobile devices are outside the scope of this documentation.

Security-sensitive customers can enable a project option that requires 2FA before entering the project. Enabling or disabling 2FA restrictions for a project is recorded in the project log. LMC-managed principals who cannot provide a second factor, or whose shared secret was generated by different software, will not be able to enter these projects. Principals must set up a separate TOTP generator for each LMC instance they can access, since each LMC instance generates different shared secrets for each principal.

For IdP-managed principals, the IdP must be configured according to company security guidelines. Secure IdP configuration guidelines are outside the scope of this documentation. LMC does not check MFA-related claims in the ID token provided, since industry best practice assumes IdP-managed principals are sufficiently protected to access most 2FA-restricted resources.

For LMC 2FA-restricted resources, project administrators can choose whether to (a) apply no access restrictions to a project, (b) allow only LMC-managed principals to enter the project after providing their personal second factor, or (c) require either an IdP login or the principal's personal second factor to access the account. The third option allows principals from any IdP configured in the LMC instance to enter the project, provided they also have access permissions via either direct membership or IdP authorization. For more details on IdP user management, see *Alternative authentication methods* on page 8.

To add another layer of access control for highly critical resources, additional security measures outside LMC should also be considered. These measures are not covered in this documentation.

3.3 Alternative authentication methods

3.3.1 API keys

In the LMC, several types of API keys are available. Each type has a different scope and purpose.

	SIEM API keys	Principal-bound single account keys	Principal-bound cross-account keys
Account scope	Single account	One account, including direct child accounts.	Selection of one, multiple or all accounts of a principal, also possible for sibling accounts.

	SIEM API keys	Principal-bound single account keys	Principal-bound cross-account keys
Permissions	SIEM-relevant APIs	All APIs allowed as specified by membership per account, including write options.	All APIs allowed as specified by membership per account, including write options.
Maximum lifetime	Unlimited, but regular rotation recommended	1 - 3560 days, shorter-lived keys and regular rotation recommended.	1 - 356 days, short-lived keys and regular rotation recommended.
Maximum number	One per project	Five per account per principal, 100 per principal in total.	Five per account per principal, 100 per principal in total.
Use cases	Retrieve device logs of a single account for monitoring usage, querying a specific set of SIEM-relevant APIs.	E.g. retrieve monitoring data of several child accounts; assign networks to multiple sites via API script; claim, license, and assign devices to sites via API script; mass device configuration via API script.	E.g. retrieve monitoring data of several child accounts; assign networks to multiple sites via API script; claim, license, and assign devices to sites via API script; mass device configuration via API script

SIEM API keys (Security Information and Event Management) can be issued for specific endpoints in LMC and are intended only to gather information about certain events within a single account. Any other endpoint will return a descriptive HTTP error when accessed with a SIEM API key, and these keys cannot be used to perform write or delete operations.

Only project administrators can create or revoke SIEM API keys. Project administrators must ensure that a project's SIEM API key(s) are rotated whenever a principal who had access to the project's SIEM API key(s) no longer has access to that project (see *Offboarding* on page 14).

Principal-bound API keys are tied to an individual principal and inherit (mirror) that principal's permissions within the LMC account the principal accesses using the API key. They are ideal when actions must be attributable to a specific person (for auditing, per-principal limits, or fine-grained authorization), or for personal automations such as scripts that call the API using the principal's LMC account rights. Each principal typically has their own keys, which are visible and manageable only by that principal. This supports per-principal audit trails and enables easier incident response by revoking individual keys instead of rotating a shared SIEM API key.

The scope of a principal-bound API key is selected when the key is created and can either be limited to a single account (organization or project; "single-account API key") or allow cross-account access. Single-account keys can include only one project or organization. Any principal-bound API key with access to an organization where LMC administrator inheritance is enabled also allows access—via the API key—to all child projects for principals inherited from that organization, as long as project administrators have not opted out of administrator inheritance.

Cross-account access keys may include a selection of sibling accounts or all accounts the principal is a member of, regardless of their relationship to a specific parent account. Due to their potentially broad scope, cross-account keys must be created with great care and stored securely.

By default, the number of principal-bound API keys is limited to 100 keys per principal. In addition, the number of principal-bound API keys per principal per project is limited to five.

Each creation or revocation of a principal-bound or SIEM API key is logged in the accounts the key can access. In the case of administrator inheritance, it is logged only in the organization where the key is created or revoked, but not in the child accounts. When an API key is created, the key value itself is displayed only once, so principals must copy it immediately. If this is missed, the key must be revoked and a new one created.

For each API key, principals must choose an expiry option based on scope and usage:

- Because SIEM API keys grant only a limited set of rights for this purpose, they are not intended to expire automatically. They can be revoked by a project administrator at any time. Nevertheless, we strongly recommend regularly revoking, recreating, and redeploying SIEM API keys to reduce potential security risks.
- Principal-bound API keys with single-account scope at the project level can be valid for 1 to 365 days or set to "unlimited." However, the "unlimited" option is restricted by the LMC backend to a maximum lifetime of 3,650 days.

We strongly recommend using time-based expiry for all single-account API keys. Short-lived keys and regular rotation are considered good practice.

› Principal-bound API keys with cross-account scope are always created with a time-based, automated expiry. The expiry must be selected each time an API key is created and can range from 1 to 365 days. Short-lived keys and regular rotation are considered good practice.

Project administrators can choose to prohibit API key usage entirely for the account they are responsible for. No new API keys can be created for accounts whose administrators have opted out of API key access. Attempting to access such accounts with a key that was created before the restriction will result in an HTTP 403 (Forbidden) error.

Every account access using any API key is logged in the corresponding account log. Each management action that is typically logged in an account context is marked as having been performed using an API key.

As of December 2025, API keys cannot be created by or used by IdP-managed principals in LMC. Unless prohibited by compliance requirements, LMC allows a mix of IdP-managed and LMC-managed principals within an account. In this scenario, LMC-managed principals with personal API keys can be used for automation. API key usage must then be closely monitored by account administrators, along with any required manual principal offboarding, if applicable (see also *Manual offboarding* on page 14). Further security improvements for API key usage in LMC IdP user management scenarios are currently being investigated.

3.3.2 IdP principal management

Identity Provider (IdP)–based principal management was introduced in LMC to fulfill EU legal requirements and to simplify LMC principal management. To meet strict access-control criteria, LMC fully delegates identity proof to the IdP via the OpenID Connect (OIDC) authorization code flow with PKCE. The IdP verifies the principal's credentials (email address and password stored in the IdP) and then issues a signed ID token, which LMC validates and uses to establish a local session for the principal identity. After the principal's identity is verified, LMC's built-in session management is applied.

Currently, Microsoft Entra ID (OIDC v2 endpoints), Keycloak, Okta/Auth0, OpenText Access, and Ping Identity have been proven to work. We expect other IdPs to work as well, provided they implement the OIDC standard correctly. In this scenario:

1. Login to LMC happens through the customer's IdP.
2. LMC trusts only signed, validated responses and never sees or stores the principal's primary credentials.
3. Passwords, personal 2FA secrets, and personal API keys for principals with a specific email domain are removed when an IdP configuration for that domain is enabled, to improve security.
4. If the IdP is unresponsive, typical HTTP errors will occur. Only if the corresponding IdP configuration is disabled by an account administrator can principals of the affected domain use the "Forgot password" function on the LMC login screen to regain access. This works only as long as the IdP configuration for that domain remains disabled. If it is re-enabled, LMC will again remove any passwords, second factors, and principal-bound API keys those principals may have set up or created in the meantime.

To enable IdP authentication for principals of a specific domain, the corresponding IdP configuration can be created in any LMC account. Any change to the configuration is recorded in that account's log.

With IdP principal management and authentication enabled for a domain, principals in that domain can create LMC principals on their own by:

1. Accessing the LMC login page
2. Completing the IdP authentication
3. Returning to LMC for the first time and accepting the principal Terms of Use document provided
4. If the IdP configuration for the domain is set up for authentication only, account administrators must send account invitations to those principals so they can access the account with the role granted by that invitation.

In addition, LMC can be configured to determine which authority a principal is granted based on authorization data provided by the IdP and mappings configured in LMC. In this case, the IdP supplies identity plus coarse-grained signals (groups/roles), which are mapped to an LMC authority. Fine-grained checks are enforced by LMC's own RBAC rules on every UI or API operation, using the established principal identity and the account context. For these principals, LMC memberships do not take effect, and no memberships are stored for the principal. This ensures that a principal is granted

only the rights derived from the current session's ID token. It is not recommended to assign additional direct memberships to these principals in the IdP-authorized account (or its account hierarchy), as direct memberships would override rights granted by the IdP. Direct memberships for IdP-authorized principals can, however, be created at any time in sibling accounts to grant access outside the IdP-authorized account (or account hierarchy).

As of December 2025:

- Only one LMC authority can be assigned per principal via IdP group/app-role mapping, resulting in a single role (e.g., a project role) across all projects the principal can access.
- Multiple IdP groups can be mapped to the same LMC authority.
- An IdP group/app role can be left blank for either the organization or project mapping. In that case, principals with that IdP group/app role will have no access at the account level where the LMC authority mapping is blank.

Whenever an IdP user account is disabled, or the corresponding group membership/app role changes in the IdP, the next LMC login (or session validation) will result in updated authorities—or access revocation—in LMC.

3.4 Session security

Authentication and authorization in LMC are based on signed JSON Web Tokens (JWTs). Using the signing mechanism, other microservices can validate the integrity of the information contained in a token. Browser instances used by principals (clients) can call a dedicated endpoint to obtain new access tokens, either by using a username and password or by using existing tokens. Once issued, the client can use the token (within the predefined time frame) to prove that they are authenticated and authorized to access the requested business logic. This is done by including the token in the header of each request.

This approach has several implications for the user experience:

- To provide a seamless experience, a single LMC UI session can be shared across multiple tabs within the same browser instance.
- Closing the browser will not end the LMC session unless the session times out in the meantime.
- Opening a second window of the same browser will not require the principal to log in again.
- Opening a different browser (e.g., Firefox in addition to Chrome/Edge) or the first incognito/private tab in a browser instance requires the principal to create a new LMC session by logging in to LMC.
- Active LMC sessions are also shared across incognito/private tabs within the same incognito/private browser instance.
- All points above also apply to IdP-managed principals.
- In environments with shared devices, it is strongly recommended to log out of LMC and close all LMC browser tabs before leaving a device unattended. Security measures to protect the device or the operating system itself are outside the scope of this documentation.
- To prevent LMC sessions from being extended indefinitely, principals can configure in their profile how long an active session should be kept alive by the LMC UI. The default is 30 minutes, but it can be reduced to, for example, 5 minutes, or increased up to a maximum of 12 hours. For typical business use cases, we recommend keeping the default of 30 minutes.

IdP session handling follows the same principles as described above.

4 Logging

Logging in LMC is available in several places, and access to logs is restricted to specific principal roles (Organization Administrator at the organization level; Project Administrator and Technical Administrator at the project level). Each log entry is created while the corresponding action is processed in the LMC backend. Log messages use different templates depending on the event type and the language (English or German). Each service provides its own translation templates for the applicable message types. Log entries themselves cannot be modified by any LMC principal, automation principal, or by the service that created the entry. Database-level log entry protection is outside the scope of this documentation.

4.1 Audit logging

Account audit logs at the distribution, organization, and project levels are stored for 365 days. After that, the corresponding database entries are deleted by automated database jobs. Only account administrators, or project technical administrators, can access account audit logs.

Typically, actions performed in project settings or on management pages are audit-logged, for example:

- Creation or deletion of principal accounts
- Creation or revocation of API keys
- Principal logins to the account (including IdP-managed principals)
- Changes to a principal's memberships within an account
- Enabling or removing a 2FA restriction for an account, or any other account security-related change
- Network creation or change events
- Device claiming, removal, or license status changes

Each account audit log entry contains at least an overview section that is readable at first glance without further interaction:

- Log level and timestamp of the action
- A human-readable action type
- The email address of the principal who performed the action that resulted in the log entry

When a log entry is expanded, additional information is displayed:

- The service that created the entry
- An identifier for the affected entity (usually the name assigned by the principal) and the source of the action. The source can be the browser used to access the LMC UI; in that case, the browser type, operating system, and current LMC UI version are recorded.
- If automation is used to perform an action, the IP address that issued the request is recorded, as well as the tool used to trigger the action, if known.

Audit log access via API keys is restricted to principal-bound API keys of LMC-managed account administrators and project technical administrators (see also *Alternative authentication methods* on page 8).

4.2 Device logging

Device logs can be accessed at the project level only by Project Administrators, Technical Administrators, and Project Members. To view a device log, the corresponding device must be selected and the configuration pages opened. Each device log entry contains at least an overview section that is readable at first glance without further interaction:

- Log level and timestamp of the action
- A human-readable action type
- The email address of the principal who performed the action that resulted in the log entry. If an action was performed via the device's local configuration interface, the value "system" is shown instead of the LMC principal's email address.

When a log entry is expanded, additional information is displayed:

- The service that created the entry
- The device ID
- The device name and any changed device configuration values (if applicable)

Device logs can also be retrieved automatically using either SIEM API keys or principal-bound API keys (see also *Alternative authentication methods* on page 8).

5 Offboarding

To ensure that an LMC principal can no longer access resources belonging to a specific customer after an employee leaves the company, there are generally two ways to separate concerns in this case.

5.1 Manual offboarding

Offboarding LMC-managed principals requires manual steps performed by an account administrator (at the distribution, organization, and project levels, as applicable). These actions must be completed for each principal who should no longer have access to LMC and include the following steps:

1. Remove all memberships from all accounts the principal can access.
2. Remove direct memberships from any child accounts of organizations with administrator inheritance enabled that the principal can access due to administrator inheritance and for which the principal also accepted an invitation.
3. Revoke the principal's personal API keys.
4. Rotate SIEM API keys for projects the principal can access.
5. Change device and hotspot passwords for accounts the principal can access.
6. Deleting the LMC principal itself is also recommended. This can be done only by the person who owns the principal via their principal profile section, or by submitting a special, documented request from the company that owns the account to the LMC Support competence team (requires a request and documentation in Support Jira).

5.2 Offboarding for IdP-managed principals

Offboarding for IdP-managed principals requires less manual work than offboarding LMC-managed principals, but it must be performed with the same level of attention.

1. For any person with LMC access who (a) no longer works for a company or (b) changes responsibilities within that company, the company's IdP administrators must update the principal's IdP configuration so that LMC no longer receives a positive result during login.
2. On every login attempt, LMC checks the IdP configured for the principal's email domain to verify whether the principal is still active, valid, and exists in that IdP.
   a. As long as this check succeeds, the principal is allowed to sign in to LMC.
   b. If this check fails, access to LMC is denied.
3. In addition, we strongly recommend periodically reviewing and adjusting:
   a. All principals' LMC access and granted rights, whether managed in LMC itself or in the IdP.
   b. Whether administrator inheritance is still needed for an organization or a specific principal, and whether any direct project memberships for initially inherited administrators are still required (if applicable).

For IdP-authenticated principals, LMC stores direct memberships. Please pay close attention to the following: **Even if IdP principal authentication is enabled, always manually remove a principal's memberships to prevent password-reset bypasses if an IdP configuration is disabled by an account administrator.**

For IdP-authorized principals, access rights are also granted based on values returned by the IdP. In this case, LMC does not store any memberships, so disabling the principal—or removing the principal's rights—in the

responsible IdP is sufficient to effectively block the principal's access to LMC. **Nevertheless, any direct memberships for IdP-authorized principals must also be removed manually.** Deleting the LMC principal itself is optional and must be done as described above.