Application Permissions and Security

Luware
Nimbus

Luware

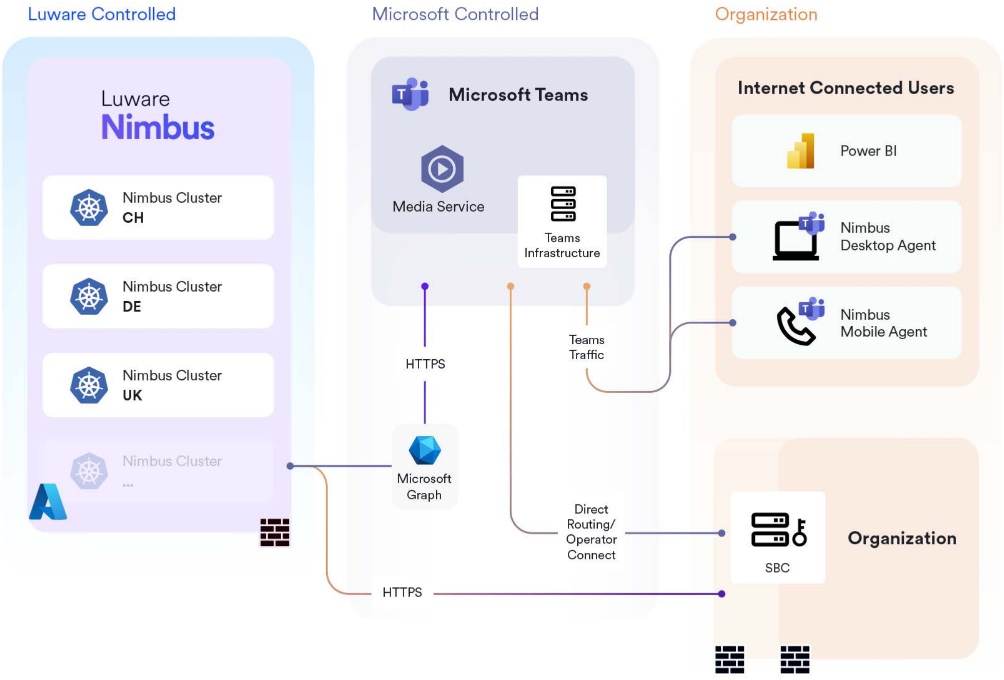
Table of Contents

1 Luware Nimbus Overview

1.1 Application Landscape

Luware Nimbus is Contact Center as a Service (CCaaS) solution with a modular set of applications that can be combined to create a unique contact center solution. It's main components are:

- **Microsoft Teams:** Acting as the host system within your customer M365 tenant, Microsoft Teams provides the foundation for Luware Nimbus.
- **Microsoft Azure:** With clusters strategically located in Switzerland, the UK, and Germany (EU), Luware Nimbus leverages Microsoft Azure for a robust and reliable performance.
- **Graph API:** Luware Nimbus seamlessly integrates with the Graph API to use the Teams Phone system for all contact center calls and call control experiences.
- **PowerBI:** Integrating with Power BI, Luware Nimbus provides advanced analytics and reporting capabilities.
- **Power Automate:** Through a Power Automate connector, Luware Nimbus integrates and automates processes between applications**.**



Luware Nimbus is hosted in Microsoft's Azure cloud service infrastructure and harnesses Microsoft's Bot Services and APIs to integrate into the Microsoft ecosystem. Luware Nimbus's environments are configured to harness Azure's traffic and load management toolset and are distributed across multiple geographic regions to enable organizations to comply with their local cloud regulations.

For user authentication, application/infrastructure monitoring, logging, and security, Luware relies on Azure-native services. These are further enhanced for the operational management of the service through additional tooling built into Luware Nimbus. The customer's Azure tenant has all the necessary applications to use Power Automate, access the OData interface, and grant access to the Nimbus application.

1.2 Luware Nimbus Application Components

The components can be divided into three general blocks:

- Components hosted in the customer’s tenant
- Luware Nimbus Assistant as a Windows application installed on the user’s workstation
- Components hosted in the Luware tenant

The components listed on the Luware tenant provide the interface needed to, for example, access reporting data or connect with the Luware Nimbus Assistant.

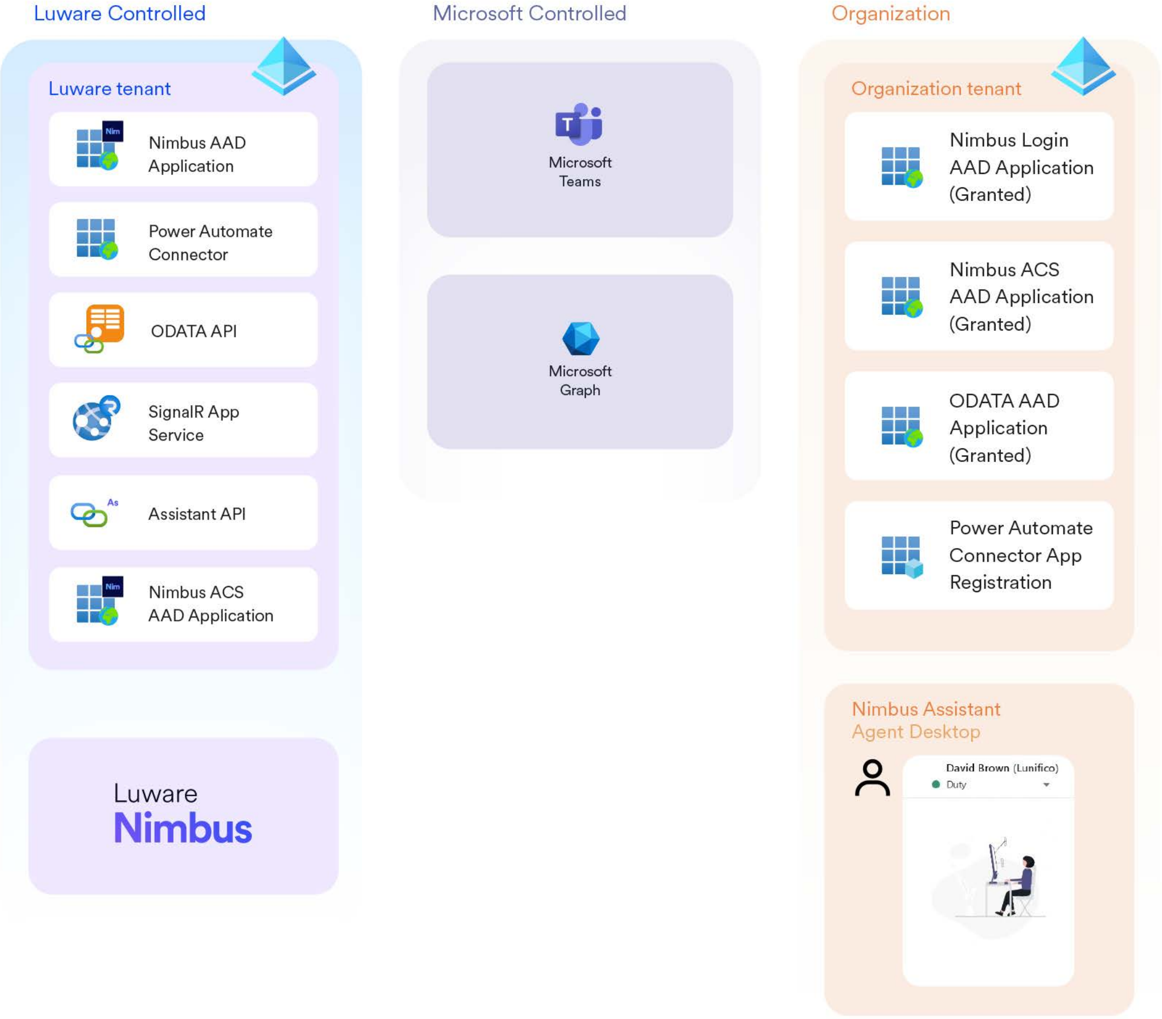
1.2.1 Components Hosted on the Organization’s Tenant

Luware Nimbus Login: An enterprise application hosted in Azure Active Directory.

Luware Nimbus ACS: An optional enterprise application. If this application is not available, a default connection to ACS is established (Luware ACS connection string is used). If configured, the connection string from your enterprise application must be registered in the tenant settings and will be used in Nimbus Assistant and Instant Messaging.

OData AAD: An optional enterprise application. If you want to access the OData interface (reporting) to extract data for further use, you will need to register this enterprise application in your tenant.

Power Automate AAD: An optional enterprise application. If you want to access third-party applications with Power Automate, you must register this enterprise application in your tenant.



The organization's tenant and the Luware tenant communicate via the GraphAPI. Luware Nimbus (as a custom application) requires some permissions from the organization's tenant to enable full functionality. Luware Nimbus also delegates some permissions to the logged-in user where appropriate. The Luware Nimbus applications run within a Microsoft Teams resource account.

1.3 Application Permissions in Luware Nimbus

In Azure AD, there are two types of permissions: “Delegated” permissions and “Application” permissions.

- "Delegated” permissions use user credentials. Access is primarily limited by the permissions assigned to the user account. To access Microsoft Teams data, the user must have the correct permissions within Teams. Delegated permissions are intended for interactive sessions, such as when you run commands in PowerShell on the fly.
- "Application" permissions use Azure AD App Registrations / Service Principals for authentication. Access is strictly defined by which API scopes have been configured for that Service Principal in Azure AD, and which have been approved by an administrator. Application permissions are a bit more complex to set-up, but are intended to be used by automated processes, such as data collection for reports.

For more information about these two types of permissions, please refer to this overview.

1.3.1 Required Application Permissions

Each time, the Microsoft Power Shell script is run to provision a new Luware Nimbus service, the following components are created / updated:

Component	When permissions are granted	Description
Nimbus App	On each run of the script	Gets information about Teams users, their team memberships and roles, and group memberships
Calling Bot	On each run of the script	Responsible for the team calls (regardless of team/workflow configuration)
Media Bot	On each run of the script	Enables voice message recordings
Chat Bot	In User Preferences (Portal) once by the user to register with the bot. No additional permissions are needed.	Relay service-related chat messages via adaptive cards

The Microsoft.Graph.* modules which are used by the provisioning script require permissions that need to be granted for the Microsoft Graph PowerShell enterprise application:

Permission	Type	Granted By	Purpose
Application.ReadWrite.All	Delegated	Tenant Admin	Read and write all applications
AppRoleAssignment.ReadWrite.All	Delegated	Tenant Admin	Manage app permission grants and app role assignments
DelegatePermissionGrant.ReadWrite.All	Delegated	Tenant Admin	Manage all delegated permission grants
Domain.Read.All	Delegated	Tenant Admin	Read domains
Organization.Read.All	Delegated	Tenant Admin	Read organization information
Users.ReadWrite.All	Delegated	Tenant Admin	Read and write all users' full profiles
openid	Delegated	Tenant Admin	Sign users in
profile	Delegated	Tenant Admin	View users' basic profile
offline_access	Delegated	Tenant Admin	Maintain access to data you have given it access to

1.3.2 Detailed Permissions by Products / Features

The Call.* permissions are used by the Luware Nimbus Calling Bot application and are required to be able to participate in calls and to control them.

Luware Nimbus runs as a host application within Microsoft Teams. When a call comes into Teams and is directed to Luware Nimbus, Teams invites the Luware Nimbus Calling Bot to join and control the call.

The following permissions are application permissions:

Permission	Type	Granted by	Advanced Routing	Enterprise Routing	Contact Center	Attendant Console	Interact	Nimbus Assistant
Calls.AccessMedia.All	Application	Tenant Admin	✓	✓	✓	✗	✗	✗
Calls.Initiate.All	Application	Tenant Admin	✓	✓	✓	✗	✗	✗
Calls.InitiateGroupCall.All	Application	Tenant Admin	✓	✓	✓	✗	✓	✗
Calls.JoinGroupCall.All	Application	Tenant Admin	✓	✓	✓	✗	✓	✗
Channel.ReadBasic.All	Application	Tenant Admin	✓	✓	✓	✗	✗	✗
GroupMember.Read.All	Application	Tenant Admin	✓	✓	✓	✗	✗	✗
OnlineMeetings.Read.All	Application	Tenant Admin	✗	✗	✗	✗	✓	✗
OnlineMeetings.ReadWrite.All	Application	Tenant Admin	✗	✗	✗	✗	✓	✗
User.Read.All	Application	Tenant Admin / Nimbus App User – Nimbus UI	✓	✓	✓	✗	✓	✗

Permission	Type	Granted by	Advanced Routing	Enterprise Routing	Contact Center	Attendant Console	Interact	Nimbus Assistant
Presence.Read.All	Delegated	Tenant Admin	✓	✓	✓	✗	✗	✗
User.Read	Delegated	Tenant Admin	✓	✓	✓	✗	✗	✓
User.ReadBasic.All	Delegated	Tenant Admin	✓	✓	✓	✗	✗	✗
Calendars.Read	Delegated	User	✗	✗	✗	✓	✗	✗
Calendars.Read.Shared	Delegated	User	✗	✗	✗	✓	✗	✗
Contacts.Read	Delegated	User	✗	✗	✗	✓	✗	✗
Contacts.Read.Shared	Delegated	User	✗	✗	✗	✓	✗	✗
Presence.Read.All	Delegated	User	✗	✗	✗	✓	✗	✗
User.Read	Delegated	User	✓	✓	✓	✗	✗	✗
User.ReadBasic.All	Delegated	User	✓	✓	✓	✗	✗	✗
Teams.ManageCalls	Delegated	User	✗	✗	✗	✗	✗	✓

Permission	Type	Granted by	Advanced Routing	Enterprise Routing	Contact Center	Attendant Console	Interact	Nimbus Assistant
Teams.ManageChat	Delegated	User	✗	✗	✗	✗	✗	✓
User.Read.All	Delegated	Tenant Admin	✗	✗	✗	✗	✗	✓
Presence.Read	Delegated	User	✗	✗	✗	✗	✗	✓

A detailed description of all permissions by products / features can be found in the Luware Knowledge Base.

1.4 Additional Information to the Application Permissions

Luware Nimbus requires permissions within Microsoft Graph to enable basic functionality such as call distribution, displaying and using presence information, but also for displaying caller information. These permissions are only used in connection with Luware Nimbus calls and/or chats. Without these permissions, Luware Nimbus will not work.

Detailed description of the Microsoft application permissions can be found on the Graph permission reference website as well as on the Azure AD API permission description website.

1.4.1 Calls.AccessMedia.All

There are two situations where application permission is used: In IVRs, the caller can select options using DTMF tones. If the permission is not set, the IVR would not work.

If we want to record a voicemail, we also need this permission.

This permission is only used in the Luware Nimbus application.

1.4.2 Calls.Initiate.All

This permission must be set to allow the calling bot to distribute calls. It is only used by the Luware Nimbus application for Luware Nimbus related calls.

1.4.3 Calls.InitiateGroupCall.All

This permission is used to distribute calls. It is only used by the Luware Nimbus application for Luware Nimbus related calls.

1.4.4 Calls.JoinGroupCall.All

This permission is used to join a call within the Luware Nimbus environment.

For Luware Nimbus to work, **a conference session is required** to which the caller, the Luware Nimbus Calling Bot, the selected user, and any transfer targets can be invited. For a “direct” distribution type, the selected Luware Nimbus is first called via a normal peer-to-peer connection. When he or she answers, the call gets "escalated" to the Luware Nimbus conference. In Microsoft Teams (and earlier SFB) this has always been the case - most calls start peer-to-peer between two people, but as soon as certain features are used, such as PowerPoint sharing, or when more people are added to the call, a conference is set-up in the background and the call is redirected there. The transition is barely noticeable.

1.4.5 Channel.ReadBasic.All

Read channel names and channel descriptions, on behalf of the signed-in user. This permission is used to enumerate existing channels. It enables the Luware Nimbus application to find the appropriate channel to post a voice message as an adaptive card within a channel.

1.4.6 GroupMember.Read.All

This permission allows the app to list groups and read basic group properties. It is used in Luware Nimbus to read the membership of all Luware Nimbus enabled Microsoft Teams services.

1.4.7 Online Meetings.Read.All

If you use Luware Nimbus Interact this permission allows Luware Nimbus to read the online meeting details of the active meeting.

1.4.8 OnlineMeetings.ReadWrite.All

If you use Luware Nimbus Interact this permission allows Luware Nimbus to read and create an online meeting.

1.4.9 User.Read.All

This permission is used by the Luware Nimbus application to retrieve caller information – if available. Additionally, it is used by the Luware Nimbus user interface to enable a full search for users. Luware Nimbus reads the complete profile of all users to determine group memberships within the organization. Luware Nimbus needs this information to correctly identify users via search. The presence status of Microsoft Teams users is also determined this way, which is used for call distribution.

Luware Nimbus does not store any of the exchanged data. The permissions are primarily used to display live data during daily usage of the product.

1.4.10 Presence.Read.All (delegated)

This optional permission will be used if presence tracking for external Azure guest accounts is enabled and enables Luware Nimbus Attendant Console to show the presence state in the contact search.

Allows the application to read presence information of all users in the directory on behalf of the signed-in user. Presence information includes activity, availability, status note, calendar out-of-office message, timezone, and location.

1.4.11 User.Read (delegated)

This optional permission will be used if presence tracking for external Azure guest accounts is enabled.

1.4.12 User.ReadBasic.All (delegated)

This optional permission will be used if presence tracking for external Azure guest accounts is enabled. It allows Luware Nimbus to read a basic set of profile properties of other users in your organization on behalf of the signed-in user. This includes display name, first and last name, Email address, open extensions, and photo. Furthermore, it allows Luware Nimbus to read the full profile of the signed-in user.

1.4.13 Calendars.Read (delegated)

This permission is used within the Luware Nimbus Attendant Console to read the calendar of the logged-in user with existing appointments.

1.4.14 Contacts.Read.Shared (delegated)

Allows the Luware Nimbus Attendant Console to read events in all calendars that the user can access, including delegate and shared calendars.

1.4.15 Contacts.Reamd (delegated)

Allows the Luware Nimbus Attendant Console to search the Exchange contacts of the logged-in user.

1.4.16 Contacts.Read.Shared (delegated)

Allows the Luware Nimbus Attendant Console to read contacts that the user has permissions to access, including the user's own and shared contacts.

1.4.17 Teams.ManageCalls (delegated)

Enables the Luware Nimbus Assistant to manage calls through ACS.
Start, join, forward, transfer, or leave Teams calls and update call properties as the logged-in user.

1.4.18 Teams.ManageChats (delegated)

Create, read, update, and delete 1:1 or group chat threads on behalf of the signed-in user. Read, send, update, and delete messages in chat threads on behalf of the signed-in user.

1.5 Additional Information to the required permissions by application

1.5.1 Enterprise App – "Luware Nimbus":

Application-level permissions needed by Luware Nimbus to retrieve information about configured Microsoft Teams groups and users:

- **GroupMember.Read.All**
  Allows listing all groups, their basic group properties and their memberships. This permission is not used to query all groups in a tenant. It is only used to query the group membership of two things:
  - Membership in Microsoft Teams-based teams that have been specifically enabled for Luware Nimbus Routing services (via their Team/Group ID, which is communicated when an administrator adds the Luware Nimbus custom application as a new tab to an existing team).
  - Membership in a customer-defined, dedicated security group that determines who can be a Luware Nimbus tenant Administrator with full access to all Luware Nimbus services and configuration objects (again, based on the group ID that must be manually provided by the customer).
- **Channel.ReadBasic.All**
  Allows reading channel names and descriptions for a known Team (based on the Teams' ID).

This is required to identify which channels are available for posting adaptive cards. Luware Nimbus can only query the channels of Microsoft Teams-based teams that are enabled for a Luware Nimbus Routing service.

- **User.Read.All**
  Allows reading the full set of profile properties, reports, and managers of users in the organization. This is required to retrieve and display caller information (which could be potentially any internal Microsoft Teams user from an organization), as well as information about directly or indirectly added Luware Nimbus agents. Users are identified via their User IDs, which are supplied to Luware Nimbus via Graph for inbound calls, or through query results using the above mentioned GroupMember.Read.All permissions, or directly by Luware Nimbus administrators during the configuration of Luware Nimbus agents.

1.5.2 Enterprise App – “Luware Nimbus Login”:

Delegated-level permissions to view and perform actions on behalf of the logged-in user via Luware Nimbus User and Admin Portal web pages.

It is recommended to grant these permissions on behalf of the entire organization, otherwise each Luware Nimbus user will have to request them individually (and possibly wait for an administrator to approve them first). They are used only on behalf of the user logged in through the application when accessing the Luware Nimbus Admin Portal web pages, or for keeping track of user presence states through Luware Nimbus guest accounts. Users who are not part of a Luware Nimbus service or admin group will not be allowed to access the Luware Nimbus Admin Portal pages.

At minimum:

- openid
- profile
- User.Read
  All required to allow users to authenticate (using the Microsoft authentication process) and log in to Luware Nimbus user and admin portals.

Optional:

- User.ReadBasic.All
  Retrieve basic profile information about users (used by our contact search feature within the Luware Nimbus app). Also required for Enhanced Presence Tracking via Luware Nimbus guest accounts.
- User.Read.All
  Admin-level permission – required to search for detailed profile attribute values (e.g. search by job title), which is not allowed via the User.ReadBasic.All permission
- Contacts.Read
  Allow searching the personal Exchange contacts of the logged in user (user by our contact search feature)
- Contacts.Read.Shared
  Allow searching the shared Exchange contacts accessible to the logged in user
- Calendars.Read
  Allow reading the logged-in user’s own calendar

- Calendars.Read.Shared
  Allow reading the calendar data of other users (if accessible to the user, and limited to Exchange Online calendars only)
- Presence.Read.All
  Allows viewing a contact's presence status in the contact search.
  Also required for Enhanced Presence Tracking via Luware Nimbus guest accounts.

1.6 Luware Nimbus User Interfaces

1.6.1 Luware Nimbus Teams Application

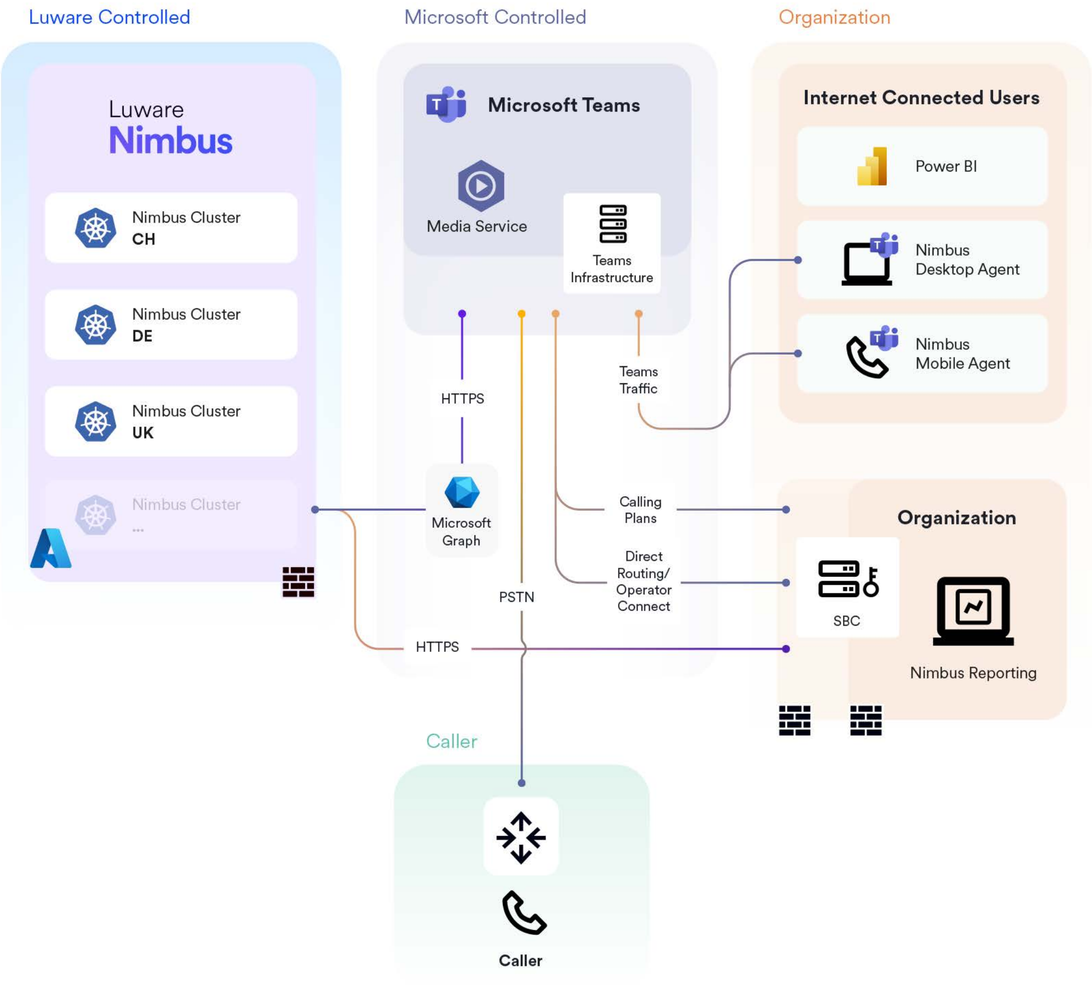
Luware Nimbus is a custom application for Microsoft Teams. It only has to be added to the corporate Teams applications admin center once by the Teams Administrator. Afterward, it becomes available to the entire organization via the Teams App Store and can be added as a new tab in any Teams channel.

1.6.2 Luware Nimbus Attendant Console

The Luware Nimbus Attendant Console extends Microsoft Teams with an intuitive call management dashboard. With the Luware Nimbus Attendant Console, receptionists and frequent callers can efficiently handle and manage incoming calls.

With the Luware Nimbus Attendant Console, users can easily log in and out of queues, view live queue information, quickly search for colleagues and see their availability, and have a range of quick transfer options, including secure and blind transfers, to distribute calls effectively.

Detailed overview of the Attendant Console including setup information.



Depiction of the call flow

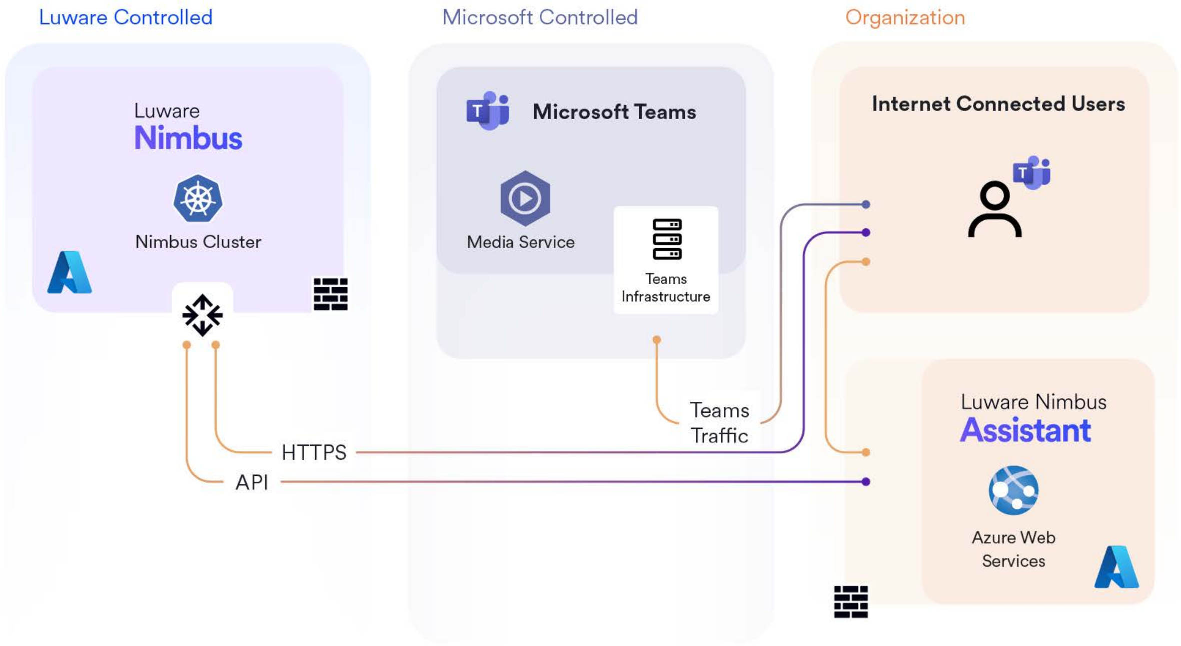
1.6.3 Luware Nimbus Assistant

The Luware Nimbus Assistant is a separate application that runs on the user's desktop, outside of the Teams platform. It uses Azure Communication Services (ACS) to connect to the Teams infrastructure and provides contextual information about incoming calls without having to keep the Luware Nimbus application open.

With the Luware Nimbus Assistant, users get an easy-to-use interface for contact center tasks such as toggling on-call status or specifying unavailable reasons, as well as triggering automated web requests such as updating tickets in an external system when receiving or answering direct or service calls.

The Assistant application itself is composed of two components:

1. A Windows application, which must be accessed to update newly added features.
2. A web application that runs within it, which is regularly updated by Luware, as it is hosted within the Luware cluster that operates in the cloud. To connect to the Microsoft Teams infrastructure, Luware Nimbus Assistant leverages Azure Communication Services (ACS).



2 Data Security and Data Privacy

2.1 Standards and Certification

Luware AG is certified for

- ISO 27001
- ISO 9001

In addition, Luware AG is currently in the process of completing the SOC 2 Type II audit report. This involves integrating the necessary security controls into Luware's daily business activities. Once the audit report is successfully obtained, both Luware Nimbus and Luware Recording will be SOC 2 Type II certified.

2.1.1 ISO 27001

ISO 27001 is an internationally recognized standard that provides a framework for establishing, implementing, maintaining, and continually improving information security management within an organization.

It is a set of guidelines that help organizations manage the confidentiality, integrity, and availability of their information assets by systematically assessing and managing risks related to these assets.

ISO 27001 provides a comprehensive approach to information security management by defining requirements for an information security management system (ISMS), including policies, procedures, and controls that ensure the protection of confidential data, such as personal data, intellectual property, and financial information.

By implementing ISO 27001, Luware AG can demonstrate their commitment to information security and provide assurance to their customers that their data is being handled securely. It also helps organizations to identify potential risks, prevent data breaches, and respond effectively to security incidents.

Overall, ISO 27001 is a valuable standard that helps Luware AG manage their information security risks and protect their valuable data assets.

ISO 27001 covers several key topics related to information security management, including:

- Information security management system (ISMS) requirements: This section outlines the requirements for establishing, implementing, maintaining, and continually improving an ISMS, which is the core framework for managing information security risks.

- Risk assessment and treatment: This section provides guidance on how to assess and manage information security risks based on a risk management approach. It includes risk assessment methodologies, risk treatment options, and risk evaluation criteria.

- Security controls: This section provides a comprehensive set of security controls, including policies, procedures, and technical measures, to protect information assets against various threats, vulnerabilities, and risks.

- Communication and awareness: This section emphasizes the importance of communication and awareness-raising activities to ensure that all employees, contractors, and third-party partners understand their information security responsibilities.

- Incident management: This section provides guidance on how to manage information security incidents, including the definition of incident management roles and responsibilities, incident reporting, and incident response procedures.

- Continual improvement: This section emphasizes the importance of continual improvement in the ISMS, including regular reviews, audits, and corrective actions to ensure that the ISMS remains effective and relevant over time.

Overall, these topics are designed to help Luware AG establish a comprehensive and effective approach to managing information security risks and protecting their valuable information assets.

2.1.2 ISO 9001

ISO 9001 is a widely recognized international standard that sets out the requirements for a quality management system (QMS) within an organization. While the standard does not specifically address data security and privacy, it does provide a framework for organizations to establish, maintain and continually improve their data security and privacy practices.

From a data security perspective, ISO 9001 requires organizations to identify, assess and manage risks related to information security. This includes implementing appropriate controls to protect against unauthorized access, theft, loss, damage, or destruction of information. ISO 9001 also requires organizations to regularly review and update their information security policies and procedures to ensure they remain effective in protecting against evolving threats.

From a data privacy perspective, ISO 9001 requires organizations to ensure the confidentiality, integrity, and availability of personal data. This includes establishing appropriate controls to ensure that personal data is only collected, processed, and used for specified purposes and that it is protected from unauthorized access, disclosure, alteration, or destruction. ISO 9001 also requires organizations to obtain consent from individuals before collecting their personal data and to provide them with the opportunity to access, correct, or delete their data.

In summary, while ISO 9001 is not specifically focused on data security and privacy, it provides a framework for Luware AG to establish, maintain, and continually improve their data security and privacy practices, which are crucial for protecting sensitive information and maintaining the trust of customers, employees, and stakeholders.

2.1.3 SOC 2 Type II

SOC 2 is a report based on the AICPA's Trust Services Criteria (TSC) that focuses on the data security aspects of a service organization's systems and processes. It provides an independent, third-party assessment of the controls that an organization has implemented to protect the security, availability, processing integrity, confidentiality, and privacy of customer data

Luware will be audited within the scope of the anticipated trust service criteria for **security**:

1. Security: The security category evaluates the effectiveness of an organization's security controls in protecting against unauthorized access, disclosure, and destruction of customer data. It includes control objectives such as access controls, encryption, network security, and physical security.

Overall, a SOC 2 audit provides customers with assurance that Luware AG has implemented effective controls to protect the security, of their data with regards to Luware's Recording and Nimbus cloud solutions. By achieving compliance with the Trust Service criteria for security, a Luware will demonstrate its commitment to data security and its ability to safeguard customer data against various threats and risks.

2.1.4 STAR Registry

As part of its commitment to provide transparency regarding its security measures, Luware AG has also published the relevant information in the Security, Trust, Assurance, and Risk registry.

The Registry is based on the CSA Cloud Controls Matrix (CCM), a cybersecurity control framework for cloud computing. It consists of 197 control objectives organized into 17 domains covering all key aspects of cloud technology. It represents a systematic assessment of Luware AG's cloud implementation and shows which security controls have been implemented within the cloud supply chain. The controls framework is aligned with the CSA Security Guidance for Cloud Computing and is considered the de facto standard for cloud security assurance and compliance.

2.2 Data Privacy

This chapter outlines the primary measures Luware AG is taking to ensure data privacy, access control, and segregation.

2.2.1 Data Locations

Luware Nimbus instances are hosted in Microsoft Azure datacenters located in different regions (Switzerland, UK, and Germany).

2.2.1.1 Switzerland

The Luware Nimbus instance Switzerland is hosted in the Microsoft Azure datacenter in Switzerland, with the primary datacenter being Microsoft Azure Switzerland North (Zurich) and the secondary datacenter (DR, backup location) being Microsoft Azure Switzerland West (Geneva).

2.2.1.2 Germany West Central

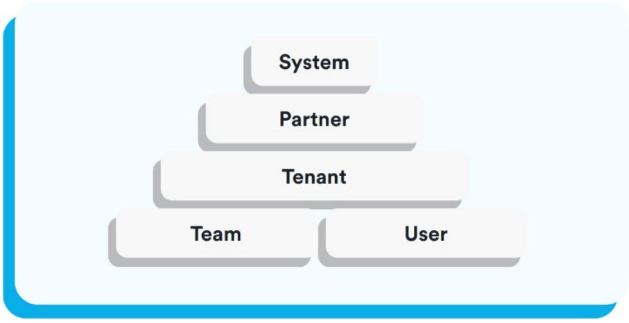
The Luware Nimbus instance Germany West Central is hosted in the Microsoft Azure datacenter located in Germany, with the primary datacenter being Microsoft Azure Germany West Central (Frankfurt) and the secondary datacenter (DR, backup location) being Microsoft Azure Germany North (Berlin).

2.2.1.3 United Kingdom

The Luware Nimbus UK instance is hosted in the Microsoft Azure datacenter in the UK, in the Microsoft Azure UK South datacenter (London) and a geo-redundant Nimbus instance is hosted in the Microsoft Azure UK West datacenter (Cardiff).

2.2.2 Data Access Types

Luware uses the following domain concept:



2.2.2.1 Luware Administrative Data Access

Luware implements the principle of least privilege and 'need to know' to minimize the risk of data exposure. Luware personnel are only authorized to access the data they necessarily and reasonably must have access to, to fulfil their current job role and responsibilities. Data access is reviewed on a regular basis to remediate any unnecessary access privileges. Requests for additional access follow a formal access request process.

2.2.2.2 Partner Administrative Access

Integration partners receive access to the system for the management of their customer's Luware Nimbus environment. Data access, administrative roles and privileges are managed by the partner administrators. It's the partner's sole responsibility to maintain and control the access scope within their own organization and for their customer's tenants.

2.2.2.3 Customer Administrative Access

Direct or end customers can also receive access to the system for the management of their Luware Nimbus environment (tenant). Data access, administrative roles and privileges are managed by the customer own administrators. It's the customers sole responsibility to maintain and control the access scope within their own organization and for their customer's tenants.

2.2.2.4 Customer Access

Data access, administrative roles and privileges are managed by the customer own administrators. It's the customers sole responsibility to maintain and control the access scope within their own organization and for their customer's tenants.

2.3 Access and Authentication

The Luware Nimbus platform is a licensed-user only system, where only specific, named individuals or members of a licensed team are given access to consume the service.

2.3.1.1 Authentication

User access is authenticated with tight integration to Microsoft's global identity management platform (Azure Active Directory - AAD) and industry standard authentication. Luware recommends OAUTH 2.0 authentication with Azure Active Directory.

2.3.1.2 Anonymous Access

Anonymous access is not supported.

2.3.1.3 Multi-Factor Authentication

Multi-factor authentication (MFA) is recommended and can be enabled by customers. This is achieved by leveraging Microsoft's Azure MFA system integrated in AAD (Azure AD) or ADFS (Active Directory Federation Services). Currently, we do not support any other multi factor authentication providers.

2.3.1.4 Role Based User Access

Administrative users that require access to operate the platform (both from a customer perspective and Luware systems administration) must have their administrative permissions explicitly granted and are only given the minimal level of access enforced via Role-based Access Control (RBAC). The customer, or their technology partner, performs self-administration of access to data by leveraging predefined Role Based Access Control policies provided by the Luware cloud products.

2.3.1.5 Generic User Accounts

Generic service and administrative user accounts are not allowed. End customer users are only ever ourensures that Luware customers maintain complete control over their user account security in accordance with their organizational requirements.

2.3.1.6 Application Service Accounts

All internal application service accounts are provisioned on a per-application basis, with enforcement of minimal permissions. Service Account details are protected, conforming to industry security standards. Example for those Service Accounts:

- Power Automate User
- PowerBI User

2.3.1.7 Presence Accounts

For an extended status presence such as "Busy → In a Call" or "Busy → In a Conference" instead of “Busy” we need to implement presence accounts (guest user). Without having guest users on your tenant as means to check, Luware Nimbus cannot see any extended user presence status. This presence accounts must not use multi factor authentication (MFA) to protect them. Instead of using multi factor authentication (MFA), we recommend using conditional access to secure those accounts.

[Detailed description of Extended User Presence]

3 Questions

3.1 User Context

> *The access to user data by the Luware Nimbus/Bot/App is always done in the respective user context, thus the already existing O365 permissions should still be considered?*

Certain information that the underlying Luware Nimbus application relies on, such as agent availability for call acceptance, cannot be restricted to the user's context. This type of information is accessed through the primary Luware Nimbus enterprise application, using established global application-level permissions as documented.

Conversely, other data actions, such as searching for transfer destinations or accessing colleagues' calendars, are performed within the user's domain. These are on-demand requests made through the

Luware Nimbus application or the user portal website. These requests occur while an actively logged in end user is using the application. The system performs these requests on behalf of the user using delegated permissions. These permissions ensure that only data that is accessible to the user is retrieved-nothing more, nothing less.

In addition, data from external systems such as SharePoint or Zendesk is also presented within the context of an authorized user account. This reinforces the secure handling of data in accordance with the user's legitimate access rights.

3.2 Admin Access to User Data

> *The access to the user data by the Luware Nimbus/Bot/App is always done in the respective user context, thus the already existing O365 permissions should still be taken into account. Check whether the Luware Nimbus administrators have full access to user data, since the Luware Nimbus/Bot/App provides full access, or whether only admin activities are possible.*

Luware Nimbus operates on a role-based access framework that can be effectively organized through the use of organizational units. This setup makes it easy to assign appropriate permissions to users within the Nimbus environment.

In practice, this means that a Luware Nimbus tenant Administrator has the authority to configure all necessary settings for the entire tenant. On the other hand, an Organizational Unit Administrator, equipped with a selectively configurable scope of access, can only manage settings for his designated organizational units.

In addition, access to reporting data can be controlled through specific administrator role assignments. These assignments can be fine-tuned to include only a specific subset of services or users.

However, it's important to note that permissions set through Azure, Office 365, or related systems such as Zendesk come into play when information outside of the Luware Nimbus domain is involved. As a result, the user experience is consistent with what they would see if they were logged into these other systems. In essence, the user's view is harmonized across systems.

Note: Luware Nimbus tenant Administrators have full access to the reporting data of the entire tenant - except for user state tracking data - provided via the OData interface.
Roles and Permissions

3.3 Restriction To Prevent Unauthorized Access

> *Check with Luware **how the Nimbus/Bot/App can be further restricted** to prevent unauthorized access (today, for example, no restriction to specific user groups).*

The following two concepts allow control over which actions can be performed and which data can be accessed, and give the possibility to restrict access to areas of the system:

- OUs (Organization Units)
- RBAC (Roles and Permissions)

Additional settings can be set on tenant level:

- Tenant Administration Group (Based on Azure Active Directory Group)
- Service Provisioning Settings (which allows to restrict the creation of Nimbus Services)

In this context, access monitoring on the customer side also plays an important role.

In the context of the Teams configuration, managing visibility and access to the Luware Nimbus application involves two key aspects: controlling the visibility of the Nimbus application itself and regulating the use of the underlying enterprise applications.

To control the visibility of the Luware Nimbus application, you can use application permission policies. These policies allow you to determine who can see the Luware Nimbus application within their Teams client.

You can also restrict the use of the underlying enterprise applications. This can be accomplished by assigning users or groups directly in Azure. However, it's worth noting that this approach is generally not necessary if the native Luware Nimbus role-based access control (RBAC) mechanisms are properly implemented.

For example, users will have the ability to view the Luware Nimbus application in their Teams client. However, their ability to log in and use the features of the app depends on their authorization status, which is determined by their membership in a Luware Nimbus-enabled service.

Similarly, access to the Luware Nimbus Admin Portal is subject to specific RBAC roles assigned to individual user accounts. This ensures that a user can only log in to the portal if they have the appropriate role. Once logged in, they are restricted to viewing data and changing settings that fall within the boundaries of their assigned role.

Luware