# CAMPUS NETWORK ON DEMAND DATA SECURITY AND PRIVACY

TECHNICAL WHITE PAPER

Alcatel·Lucent
Enterprise

# TABLE OF CONTENTS

# 1. ALCATEL-LUCENT ENTERPRISE CAMPUS NETWORK ON DEMAND SERVICE

Alcatel-Lucent Enterprise Campus Network on Demand Service (NoD) is a flexible service that allows our Business Partners to integrate our LAN and Wi-Fi® services into managed service offerings to their customers. Managed services offer a financial alternative for businesses that do not want or are not able to acquire these services in a capital purchase model. Campus Network on Demand allows our company to centrally meter usage of the equipment and provide our Business Partners with a centralized network management system to support customer networks.

While this new connection-oriented architecture model delivers flexibility and control, it must also ensure the highest security and privacy levels. Campus Network on Demand is built upon state-of-the-art security technologies, rigorous control measures and processes developed to deliver best-in-class data security and privacy to customers.

The high-level architecture of Campus Network on Demand relies on the interconnection of the following three main zones:

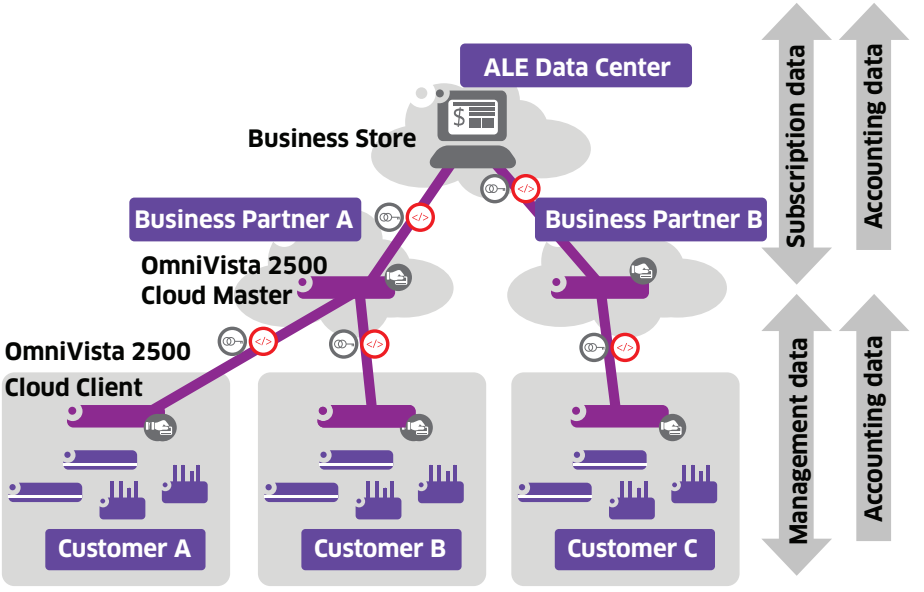
1. The Alcatel-Lucent Enterprise Business Store in our data centers
2. The Alcatel-Lucent OmniVista® 2500 Network Management System (NMS) Cloud master on the Business Partner premises
3. The OmniVista 2500 NMS Cloud client on the customer premises

The **Business Store** is a consistent, easy-to-use web portal that delivers the Campus Network on Demand application. The Business Store furnishes detailed accounting information for each subscription, and the underlying data information system managed in our data centers. The Business Store contains high-level network information, such as Business Partner information, customer information, duration and pricing. It tracks serial numbers, retrieves accounting information and provides the Business Partner with usage reporting.

On the Business Partner premises, the **OmniVista 2500 NMS** Cloud master manages the customer networks and relays accounting information.

On the customer premises, the **OmniVista 2500 NMS** Cloud client system collects management and accounting information.

Figure: Campus Network on Demand high-level architecture




These three zones are interconnected through the Internet, and all connection links are secured with strong encryption, authentication, and access controls. All individual network elements are designed to implement the technical measures described in this document.

## Data security and privacy by design

Data security and privacy are at the core of the Campus Network on Demand suite. Campus Network on Demand services ensure the highest security and privacy levels with built-in duplicate disaster recovery, physical protection of the data center on our premises, secured end-to-end data transmission, secured storage, and access controls.

Campus Network on Demand services are made up of the following four key components of data security:

- **Availability** for continuous access to data, which is critical to keeping control on the network infrastructure.
- **Integrity** in taking care that the collected data is maintained in its original state and has not been intentionally or accidentally altered.
- **Confidentiality** by ensuring that the collected data is made available or disclosed only to authorized entities and people. This principle is central to our processes and systems definition. The next sections of this document detail the control measures in place to guarantee data privacy.
- **Traceability** so that transactions, or communications, are genuine and labeled in time and origin.

These security pillars align with the core security values of our products and services:

- **Continuous security and improvement**
- **Transparency**
- **Compliancy by design** with state of the art Information System and Cloud security controls, and data privacy regulations.

## Business Store information structure for Campus Network on Demand

For delivering consistent security as an end-to-end solution, our company implements the appropriate security controls at three levels of the Campus Network on Demand architecture:

1. From the LAN and Wi-Fi facilities to the OmniVista 2500 NMS Cloud management platforms.
2. In the Business Store that holds the anonymous metering data used for Campus Network on Demand services and business applications for the Business Partner and customers.
3. At all communication interfaces that connect all these elements, from the customer premises to the Business Partners to our company.

In this architecture, we put a particular focus on end-to-end security, with measures and processes to secure both the OmniVista 2500 NMS Cloud management platforms and the Business Store with the data collection it contains. It is important to note that the Business Store data collection system is a protected and isolated system that is not exposed to any user or third-party application.

The following elements compose the data notice describing the content and key properties that give structure to the information collection performed in the Business Store for Campus Network on Demand services:

The network equipment data is collected from OmniVista 2500 NMS Cloud clients and validated by OmniVista 2500 NMS Cloud masters. The data is expanded to have separate events per available status (port, chassis, customer, Business Partner) and time-stamped by the date of reception of the data. The Business Store collects:

- The link status per type of port per hour per subscription. The timestamp is the date of compute.
- The number of associated devices per type of access point per hour per subscription. The timestamp is the date of compute.
- Information provided through the Business Store about the customer subscription and the Business Partner information.
- A common index of the project for identification.
- An inventory index to retrieve the list of pay-per-use-enabled devices per subscription associated with a Business Partner.
- A compute usage index to calculate the billing usage per type of port per device per subscription per day.

When the data is collected, the daily usage per type of port per device and access point is calculated to allow monitoring the pay-per-use activity.

For the related applicable privacy statements, please refer to Section 3.

# 2. TECHNICAL SECURITY MEASURES

The Business Store infrastructure and Campus Network on Demand processes are regularly reviewed by our operations and security teams based on a set of security control domains that comply with industry standards such as the ISO 27001/27002, ISACA COBIT, PCI, NIST, and OWASP. Our company implements the necessary controls for information security tailored to the cloud networking industry. In addition, the overall security assessment of the Business Store and OmniVista 2500 NMS Cloud equipment is completed with third-party security audits.

The implementation of the following security measures provides a strong information security baseline while maintaining business information requirements. These controls reduce and identify consistent security threats and vulnerabilities in the interconnection of Campus Network on Demand elements between the customers, the Business Partner, and our company across the Internet. We also implement standard security and operational risk management processes, and seek to deliver on industry security expectations as detailed in the Cloud Security Alliance Cloud Controls Matrix (see https://cloudsecurityalliance.org/group/cloud-controls-matrix/).

The following section provides the current security measures established by our company in the Campus Network on Demand suite perimeter. We pursue continuous improvement, keeping a comparable or better level of security. This may mean measures or controls may be replaced or redefined in order to serve the same purpose without diminishing the security level of the overall solution.

## Physical access control

Our company ensures that unauthorized people are prevented from gaining physical access to the premises, buildings or rooms that house data-processing systems that process and/or use Campus Network on Demand data.

We ensure that Campus Network on Demand data centers adhere to strict security procedures enforced by locking systems, access control mechanisms, intrusion detection systems, and other measures to safeguard security areas and their entry points against entry by unauthorized persons. Only authorized representatives have access to systems and infrastructure within the data center facilities.

## System access control

Data processing systems providing the Business Store service are protected from unauthorized use.

We apply multiple authorization levels to grant access to processing systems. The Business Store data collection system is never accessed directly by any user of the system. We have processes in place to make sure that only authorized users have the appropriate authorization to add, delete or modify the application processing the data.

All of our internal users access our systems with a unique identifier (user ID). Our standard procedures ensure that any authorization changes are implemented only in accordance with our system information security policy (for example, no rights are granted without authorization, access rights are revoked when a user leaves the company or changes roles).

The company network is protected from the public network by firewalls. The Business Store data collection system is isolated from the company network by a second level of firewalls. Security perimeters are implemented by design in the network architecture of the Campus Network on Demand end-to-end solution so that direct access to critical storage points or systems is not possible.

Our company has established password policies that prohibit the disclosure and sharing of passwords used for authentication. These policies define the measures to apply in case of disclosure, and require that passwords be changed on a regular basis. Personalized user IDs are assigned for authentication. We follow industry-standard best practices requiring that passwords are complex in length and composition.

Full remote access to our corporate network and critical infrastructure is protected with strong authentication. Direct remote access to the critical infrastructure and storage system is forbidden and these perimeters are isolated by multi-layer firewall protection architecture.

On the customer application side, Business Partners accessing the Campus Network on Demand web application or subscription services through the Business Store also benefit from a controlled role-based access login to their dedicated environment, with each user environment segregated to protect the confidentiality of data. User authentication relies on robust single-sign-on mechanisms to secure and improve the user experience.

## Data access control

Any access to personal, confidential or sensitive information is granted on a need-to-know basis to the processing application that delivers the intended services. When information is housed in the Business Store, our systems and applications can access only the data required to complete the Campus Network on Demand service. Our company utilizes authorization concepts that document how authorizations are assigned and which authorizations are assigned to the corresponding employees and related applications. All personal, confidential, or otherwise sensitive data is protected in accordance with our information system security policies and standards.

All Campus Network on Demand storage and production servers are operated in the relevant data centers and server rooms located in France. Security measures that protect applications processing personal, confidential or other sensitive information are checked regularly. To this end, our company conducts internal and external security checks and penetration tests on the IT systems to verify robustness and system integrity.

## Data transmission control

Our company implements security by design for communication technologies used to transfer data or enable communications between network equipment and systems.

Our industry-standard encryption protects Campus Network on Demand data in transit. The communication protocols rely on transport layer security (TLS) technology. TLS is configured with the latest and continually updated secured protocol versions and hardened cipher suite savoring TLS protocol version 1.2 and usage of digital certificates with SHA-256 signature hash algorithm, and explicitly avoiding obsolete protocol versions, algorithms or libraries prone to well-known attacks such as Heartbleed, POODLE, or DROWN.

After processing treatments in our data center, access to information is granted to authenticated and authorized users through the Campus Network on Demand application portal.

## Data input control

Customer and Business Partner profile information is under the control of identified and authorized user accounts defined between our company and the Business Partner through Campus Network on Demand subscription services.

The data coming from the network equipment to the Business Store through the OmniVista 2500 NMS Cloud master platform is protected. Campus Network on Demand is designed to never allow direct input, modification, or deletion of data by any of our employees or third party users. Only identified and controlled administrators have privileged access to the systems containing data for operation, administration, maintenance, and provisioning (OAMP) purposes, but with an explicit role to not process the data itself.

## Job control

Data processing is performed solely in accordance with the Campus Network on Demand related contracts and instructions in keeping with Business Partner agreements.

In keeping with our information system security policy, collected data is afforded the same level of protection as confidential information, as defined in our information classification standards.

Our Business Partners are contractually bound to respect the confidentiality of customer data. Asset management and defined appropriate protection responsibilities are explicitly identified in our company's information security charter.

## Availability control

We use available technology to protect data against accidental or unauthorized destruction or loss.

When necessary, our company utilizes backup processes and other measures that ensure the rapid restoration of business-critical systems.

To protect against principal system outages, we employ uninterrupted power supplies that ensure power availability to the data centers at any time.

We have defined contingency plans, as well as business continuity planning and disaster recovery strategies for our information systems, including Campus Network on Demand and the Business Store, for continuous availability.

## Incident management

Our IS/IT department deploys up–to-date antivirus software at company network access points and on all workstations to provide a virus intrusion protection program with available technology.

Using our company's Product Security Incident Response Team (PSIRT) processes, we proactively implement security patch management, as well as the appropriate deployment of relevant security updates, covering both the OmniVista 2500 NMS Cloud management platforms and the technical environment of the Campus Network on Demand subscriber.

## Data separation control

Data collected for different purposes and for different customers and Business Partners is processed separately.

Our company uses the technical capabilities of the Business Store to provide multi-tenancy or separate system landscapes to each application and for each customer account that is offered within an application service.

Business Partners have access only to their own environment within the Campus Network on Demand and Business Store interfaces.

### Data integrity control

Data remains intact, complete, and current during processing activities.

We implement a defense strategy in several layers as a protection against unauthorized modifications. Again, Campus Network on Demand is designed to never allow direct input, modification, or deletion of data by any of our employees or third-party users, with the exception of identified and controlled administrators who do not work with the data itself. Our strategy also employs the controls and measures described earlier in this document, such as firewalls, security monitoring centers, antivirus software, backup and recovery, as well as external and internal penetration testing.

Finally, all of these control measures and processes are reviewed regularly to prove efficient security measure integration and to allow continuous security improvement.

## 3. DATA PRIVACY STATEMENTS

Our company recognizes that it must process the personal data of Business Partners and customers in order to conduct a successful business in an increasingly electronic economy. As defined by European Union Directive 95/46/EC, this includes collecting, using, retaining, storing, accessing and/or disclosing personal data.

Our company is committed to respecting the privacy rights and legitimate expectations of our customers, Business Partners and individuals. We are also committed to protecting, to the best of our abilities, data collected by our company from unauthorized access, use, retention, storage and/or disclosure. Meeting this commitment is one of the primary management objectives for our company, for the Campus Network on Demand suite, as well as for third parties conducting business with us and on behalf of our company.

To that end, we are committed to the following principles:

### Transparency

Campus Network on Demand services do not require the storage of personal data from customers' end-users, or content data related to their traffic. We provide required notices to Business Partners or customers relating to our processing of their data (as defined above). In the particular case of Campus Network on Demand, the service delivered is for subscription management, equipment usage accounting, and network status. Our company will provide notice in the case of any service evolution.

### Choice and consent

By subscribing to the Campus Network on Demand services, our company informs Business Partners of the available choices they may have relating to the processing of their company and subscriber profile. When required, we obtain the required implicit or explicit consent. Wherever appropriate, customers and Business Partners will be informed of their available options in providing additional personal data (for example, opt-in or opt-out) that extends the legitimate purpose of the contracted service. In addition, our company will seek to obtain, where required, the implicit or explicit consent with respect to the collection, use, retention and disclosure of their data (including possible export outside of the European Economic Area).

## Data subject access

Data subjects are provided with access to their personal data for review and updates. These individuals are customer or Business Partner admin users who provide identity descriptions (names and professional addresses) to the Business Store when subscribing to the Campus Network on Demand service for identification and product shipping contact information. These individuals have the right to review their personal data and make corrections, or updates, or request data deletion where applicable. Our company has processes in place to ensure that the individual requesting review or updates to his or her personal data is the correct person.

## Proportionality

Our company processes data only for legitimate purposes necessary for delivering the Campus Network on Demand services. These legitimate purposes include the collection and processing of data that is relevant and useful for business purposes when implementing Campus Network on Demand services, and must be consistent with notices provided to the data subject, and proportional to those purposes.

## Data retention

Our company will retain collected data only for the period of time required to fulfill the permitted purposes of application and services, and in compliance with any retention periods permitted or required by applicable laws.

## Disclosure

In order to disclose data to third parties, such as our selected partners for legitimate and identified purposes, we will seek execution of a non-disclosure agreement or introduce a confidentiality clause in executed framework contracts. For the protection of confidential information, our company will require a commitment by any third parties receiving personal data to adhere to all applicable requirements of the Alcatel-Lucent Enterprise Privacy and Data Protection Policy and related procedures (please see the web link below), as well as to applicable data privacy and protection laws.

## Data protection and integrity

Our company is committed to protecting personal data from unauthorized access and use, and working to ensure the integrity of the data collected, used and stored.

Appropriate information security safeguards, in accordance with our information security policy, are used to protect both physical and electronic data, in any format or media, against unauthorized access and use, as detailed in Section 2.

## Monitoring and enforcement

Our company is responsible for monitoring and enforcing compliance with the Alcatel-Lucent Enterprise Privacy and Data Protection Policy and applicable data privacy and protection laws.

Our personnel and affiliates must comply with the Alcatel-Lucent Enterprise Privacy and Data Protection Policy and associated procedures (please see the web link below), and the applicable laws providing for the privacy rights of individuals and protection of their personal data. We have processes and procedures in place for periodically assessing and verifying compliance with these requirements.

## Management and accountability

In assigning and supporting the management and accountability of the Alcatel-Lucent Enterprise Privacy and Data Protection Policy and associated procedures, we maintain a privacy and data protection governance structure (core team) that includes the Chief Information Security Officer, the Chief Technical Security Officer and the Data Privacy Officer, and such other positions and bodies as may be required or useful. The individuals on this team have assigned responsibilities for defining, documenting, promoting and communicating the Alcatel-Lucent Enterprise Privacy and Data Protection Policy and programs, and for developing and implementing processes and procedures to ensure compliance with those policies and procedures as well as applicable privacy and data protection laws.

Alcatel-Lucent Enterprise Privacy and Data Protection Policy:

http://enterprise.alcatel-lucent.com/Privacy



Alcatel·Lucent
Enterprise