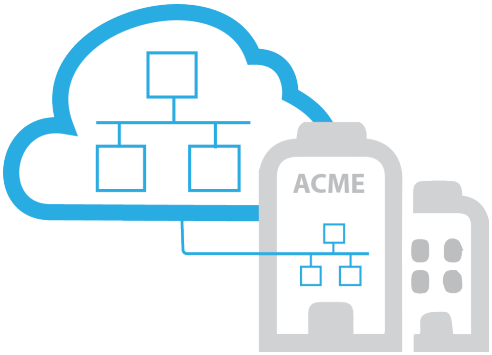
Tallac Networks

Tallac SD-BRANCH Datasheet



Tallac SD-BRANCH Remote Site Automation

Tallac SD-BRANCH is a simple, secure, cloud based solution designed to provide small to large organizations with branch locations an affordable way to deploy, and manage Wi-Fi and switch networks

Software Defined Mobility™ simplifies wired & wireless management with anytime, anywhere access directly from the cloud with easy to configure integrations and open API's for customized solutions

Orchestrate automated policies across Wi-Fi, Wired, Ethernet & Gateway devices providing intelligence in the cloud, operational decisions on the LAN

Cloud managed interface for managing the LAN with zero-touch provisioning at branch, as easy to set up and operate as Google Apps or Office 365 with no technical networking expertise needed

Secure Virtual LAN Services

- Provides distinct secure LAN services for virtual & physical services supporting mobile users, guest, VoIP, security, IoT, networked devices & applications
- Secured communication between physical network devices and Tallac SD-BRANCH Cloud through SSL and certificate validation

Simplified Management

- Zero Touch install for ease of access point deployment
- Seamlessly manage remote branches and offices behind existing firewalls
- Anytime, anywhere access for configuration and comprehensive monitoring and troubleshooting

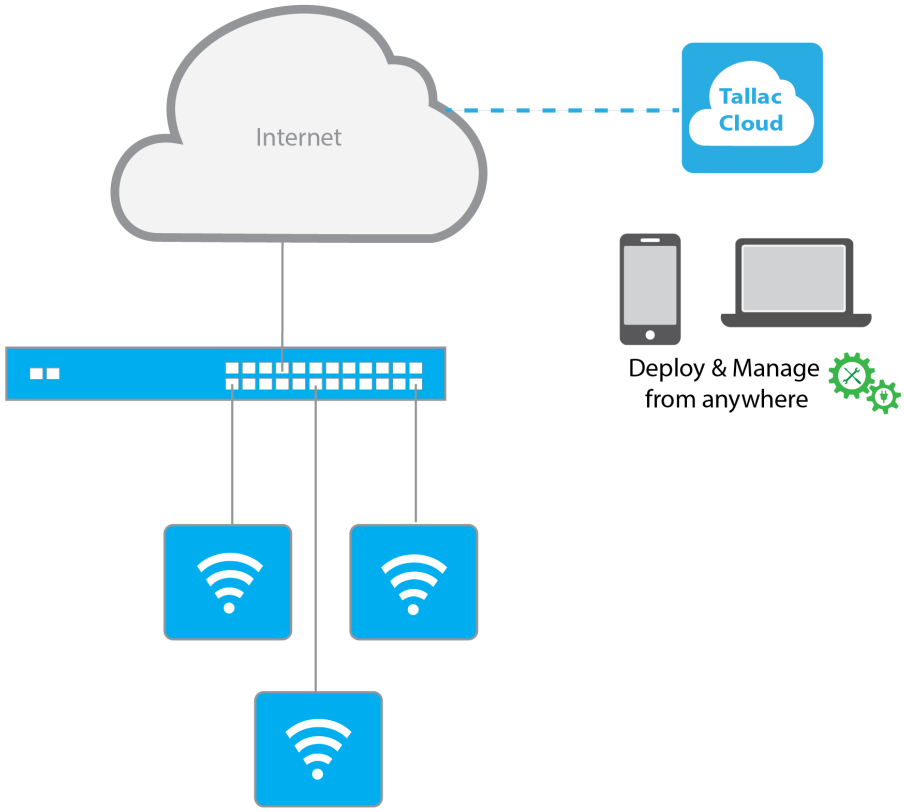
Complete wireless and wired feature set

- Support complete list of wireless security features WPA, WPA2, AAA
- Automatically adjust AP parameters by constantly monitoring the RF environment
- Control and monitor wired switch ports

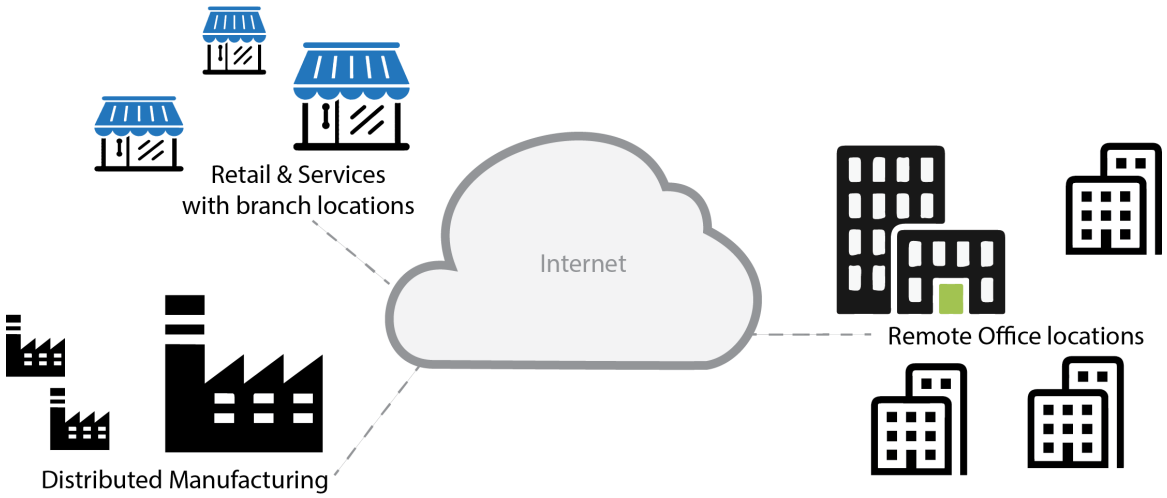
Integrate Virtual LAN services with 3rd Party Cloud services

- Pre-configured Secure Virtual LAN Integrations with 3rd party cloud services including content filtering and customized solutions
- Integrated captive portals and integrations with common authentications systems
- Fully Interoperable with SD-WAN services if present

Typical single location deployment



Common use cases for multiple locations



Ease of Management

Tallac SD-BRANCH operates using standard web browsers. With an intuitive dashboard and simple to use configuration guides, the administrator can configure and monitor single or multiple Virtual Networks across access points and switches all with a click of a mouse. Leveraging best-in-class user experience design, Tallac SD-BRANCH gives the administrators clear and comprehensive status of remote locations, and reduces the operational expenses to manage access points and switches in multiple locations.

Multi Tenancy Management

Tallac SD-BRANCH enables Managed Service Providers (MSPs), to use a single, scalable platform to manage multiple customers in a segmented and secured manner. Tallac SD-BRANCH Multi-Tenancy functionality allows a MSP to create separate multiple customer views for end users and ensure that each end user can only access devices assigned to them. The Manager view of Multi-Tenancy gives MSPs the overall status of the entire managed domain in a simple and intuitive dashboard for proactive alerts and network monitoring.

Near Limitless Scalability

Tallac SD-BRANCH is built on a distributed architecture that does not depend on a centralized controller for either the wireless traffic control plane or wireless traffic data plane management. This key differentiating characteristic allows unparalleled scalability of wireless and wired network environments without needing to upgrade or resize a wireless controller. Also, as additional resource is needed, the hosting environment automatically adds resources without the need for users to intervene.

Secured Data Flow

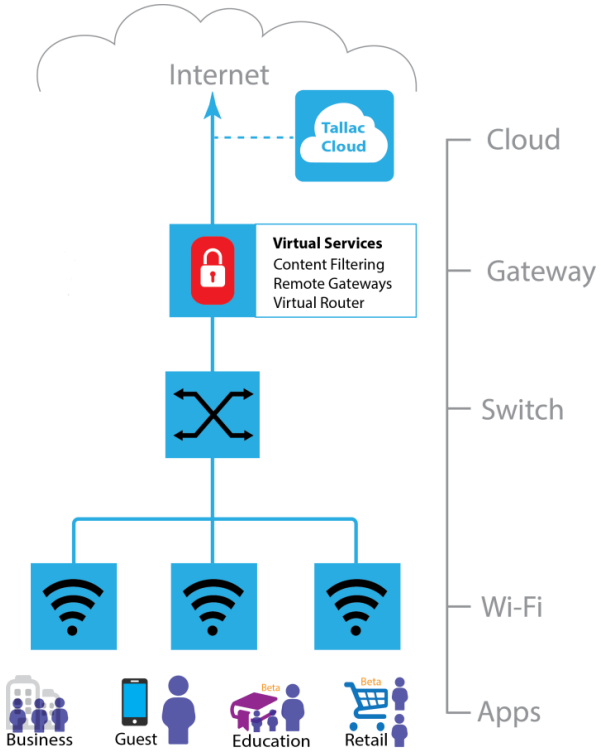
Client traffic is kept entirely on the organization's Local Area Networks. Tallac SD-BRANCH only communicates management changes (configuration, setup, administration, and reporting) and traffic monitoring reports for given access points and switches. The Tallac SD-BRANCH Cloud is out of band from the data path, intelligently and securely separating data and control traffic. While the data traffic remains in the local area network, the cloud management platform handles the control and monitors traffic independently of the data path. Following the model of Software Defined Networking, this distributed model ensures maximum scalability and ease of introducing new features and functionality independent of the access network.

Secured and Private Information Storage

Tallac SD-BRANCH follows strict rules for privacy of personal data storage. By implementing the Safe Harbor rule, Tallac guarantees that all data is securely and privately maintained with no possibility of offering data to other third parties under the strictest guideline. US-EU Safe Harbor is a streamlined process for US companies to comply with the EU Directive 95/46/EC on the protection of personal data. Intended for organizations that store customer data, the Safe Harbor Principles are designed to prevent accidental information disclosure or loss.

Encrypted Management Architecture

Control traffic between Tallac SD-BRANCH and the access points is conducted over secure connections using HTTPS. The access point verifies the authenticity of the cloud management system using a X.509 certificate. The authenticated connection uses TLSv1, encrypted with 128-bit encryption using Advanced Encryption System (AES). In addition, the data transmitted through this secure connection does not involve client data traffic.



Flexible Deployment Model

The secure connections between the Tallac SD-BRANCH and the AP's are initiated by the AP's and not by the cloud management system, thereby ensuring that the organization's firewall will not need to have a port open on inbound connections. This approach ensures that the deployment can be easily supported in all network topologies, including a NATted environment where the AP's are located behind a firewall and/or a branch gateway such as DSL or cable modem.

Redundancy and High Availability

Multiple geographically distributed data centers are used to host the Cloud Management System, thereby ensuring that the management system continues to function even in the event of a catastrophic failure of one data center. Since the Tallac SD-BRANCH is out of band for all data traffic, in the event that the organization's link to the Internet is interrupted, client data traffic will continue to flow normally — only configuration and administrative changes are temporarily impacted during an Internet connection outage. The system is automatically updated after the restoration of the Internet link.

Simplified Deployment

The provisioning of a wireless network just requires the deployment of supported access points — with setup and ongoing management undertaken inside the cloud management platform. Sizing, installation, configuration, and maintenance of a controller for management or traffic control plane is eliminated. Additional re-sizing of a controller when AP deployments grow is also eliminated.

Guest Access, Captive Portal and Logging

Guest access allows restricted access to the network, using an integrated captive portal. Three methods of entry are provided (Click-Thru, Click-Thru with email and Click-Thru with additional custom fields). Click- Thru guest access requires no authentication for the user to simply click through to access the wireless network. Click-Thru with email requires customers to enter the user email address to access the network. Click-Thru with additional custom fields option allows the operator of the Captive portal access to capture relevant user information for possibilities of targeted advertising and marketing campaigns.

Dynamic RF management

Business Central 2.0 Wireless Manager provides automatic control of access points' transmit power and channel allocation to ensure optimal coverage by minimizing channel interferences. Business Central 2.0 Wireless Manager performs scheduled automatic channel allocation to deliver an enterprise class reliable wireless experience.

Client Load Balancing

Tallac SD-BRANCH performs automatic load balancing of clients across access points to ensure even distribution of the traffic amongst the deployed APs.

SSID based Rate Limiting

Tallac SD-BRANCH provides the capability to specify uplink and downlink throughput limitation on a per SSID basis. This ensures maximum customer satisfaction by ensuring appropriate allocation of bandwidth for various services.

Choice of Gateways

Virtual networks can be configured to use the local 'Existing' physical internet gateway to reach the internet, or use a VPN to connect to 'Remote' gateway which can be hosted as a virtual cloud service. You can also configure the access point to be its own 'Tallac Gateway' and provide basic DHCP and NAT features for the Virtual Network.

Integrated Ordering

When creating a new site, or expanding an existing site users can order additional access points and switches using integrated ordering. The devices will be drop shipped to the site location and can be configured in transit for in effect zero touch installation.

Robust Wireless Security

With identity-based security features such as support for RADIUS, Active Directory and internal or external AAA server, Business Central 2.0 Wireless Manager truly unifies wired and wireless access without compromising on security. From the configuration menu of Tallac SD-BRANCH, the user can configure various wireless security settings such as WPA, WPA2, ACLs, radio parameters and push the settings to selected access points.

Technical Features

RF MANAGEMENTAutomaAutom	
Automatic Channel Allocation	• Automatic channel distribution to minimize interference • Auto-channel allocation taking into consideration the environment, interferences, traffic load and neighboring APs • Modifiable list of corporate channels to be used • Scheduled mode for Auto-channel allocation • Automatic mode in case of high levels of interference available
Automatic Power Control	• Optimum transmit power determination based on coverage requirements • Automatic power control mode available • Neighborhood scan of RF environment to minimize neighboring AP interference and leakage across floors
Load Balancing	• APs load monitoring and overloading prevention • Clients redirected to lightly loaded neighboring APs
QUALITY OF SERVICE	
WMM Quality of Service	WMM (802.11e) prioritizes traffic for both upstream traffic from the stations to the Access Points (station EDCA parameters) and downstream traffic from the Access Points to the client stations (AP EDCA parameters)
WMM Queues in decreasing order of priority	• Voice: The highest priority queue with minimum delay, which makes it ideal for applications like VoIP and streaming media • Video: The second highest priority queue with low delay is given to this queue. Video applications are routed to this queue • Best Effort: The medium priority queue with medium delay is given to this queue. Most standard IP applications will use this queue • Background: Low priority queue with high throughput. Applications, such as FTP, which are not time-sensitive but require high throughput can use this queue
WMM Power Save option	WMM Power Save helps conserve battery power in small devices such as phones, laptops, PDAs, and audio players using IEEE 802.11e mechanisms
WIRELESS SECURITY	
Client Authentication Protocols	• Open, WEP, WPA/WPA2-PSK • 802.11i/WPA/WPA2 Enterprise with standard interface to external AAA / RADIUS Server
Distinct AAA Server per Virtual Network	Yes
RADIUS Accounting Protocol	Per Client tracking for: • Bytes Tx/Rx • Login/Logout Time
Guest Access	• Click-Thru • Click-Thru with email • Click-Thru with vouchers
Captive Portal	Configurable Portal page, including image files
Rogue Access Points	• Rogue AP definition: AP with radio SSID observed by any of the Managed APs and seen transmitting on same L2 wired network • Detection and Mapping of up to 512 Rogue APs
WIRELESS NETWORK MONITORING	
Monitoring Summary	Summary of the Managed Access Points status, rogue Access Points detected, Wireless stations connected
Managed Access Points	AP status for the Managed Access Points and details that includes configuration settings, current Wireless settings, current Clients and detailed Traffic statistics
Rogue Access Points	• Rogue Access Points Reported • Rogue Access Points on same channel • Rogue Access Points on interfering channels
Wireless Clients	• Client statistics and details per AP, per SSID, per location • Trending display per hour, day, week, and month
Wireless Network Usage	Network Usage Statistics display plots of average received/transmitted network traffic per Managed Access Point