# White Paper: VANTIQ Security

## November 2017

VANTIQ

# TABLE OF CONTENTS

# Introduction

Effective digital business transformation requires increasingly powerful applications to work closely with humans to address complex situations requiring experience and intuition. VANTIQ provides the only high-productivity platform for event-driven applications focused on the rapid development and deployment of systems enabling real-time collaboration between humans and machines. Those involved in creating the next generation of digital business applications will benefit from dramatically reduced time-to-market, significantly lower development and maintenance costs, and maximum agility in response to dynamic market requirements.

Event-based applications must be secure, allowing only authorized access to the functions of the application as well as maintaining the privacy and integrity of any enterprise and personal data managed by the application. VANTIQ's comprehensive approach delivers security, integrity and privacy features spanning:

- Authentication
- Authorization
- Integrity
- Privacy
- Edge Devices
- Audit

In addition, VANTIQ operates hosted, event-based applications using secure technologies and procedures.

This document discusses these VANTIQ security features in more detail.

VANTIQ

# Authentication

Authentication guarantees that a user accessing a VANTIQ application is who they claim to be or, more precisely, that they possess valid credentials for the user they claim to be. VANTIQ supports two forms of credentials:

- Username/password pairs
- Access tokens

## Username/Password Pairs

Each user of the VANTIQ platform has a unique username. The username is associated with a password.

When presented with a valid username/password pair, VANTIQ validates the credentials. If the credentials are authentic, VANTIQ responds with a temporary access token that must be attached to each subsequent request the user issues to a VANTIQ application. The token is valid for 24 hours after which the user must again present credentials to obtain a new temporary access token. The tokens must be managed in a secure fashion within the client application or the browser session with which the user is issuing requests to VANTIQ. Even if the client application fails to protect the token, having it expire after 24 hours limits any damage that could be done if an attacker stole the temporary access token. Temporary access tokens used by client applications and browsers should be protected by observing standard policies for protecting access devices such as laptops, tablets and mobile phones.

Passwords are a common attack vector for adversaries. VANTIQ takes care to securely manage passwords. Passwords held by the VANTIQ platform are never stored as clear text. Passwords are encrypted with the latest one-way encryption technology (Bcrypt) in a computationally expensive manner using multiple hash passes. A breach of the platform's storage system yields only encrypted passwords; this discourages a brute force attack on the passwords due to the time and expense of doing so.

### Access Tokens

In some application scenarios, username/password credentials are inconvenient. For example, a utility application that performs maintenance activities on the data managed by an application may be operated by staff that should not have username/password credentials that give them general access to the data. In these cases, a long-lived Access Token may be created that is subsequently used by the maintenance application to obtain access to the VANTIQ application.

A long-lived Access Token has a lifetime specified by the administrator that created it. Therefore, the enterprise has complete control over the lifetime of the access token and the potential security exposure. Long lived access tokens may be revoked at any time by an administrator with sufficient privileges.

An application using the long-lived access token must present it on every request submitted to the VANTIQ application.

Access Tokens are available for use on both SSL/HTTPS and Secure WebSocket requests.

The specific protocol for presenting an access token to a VANTIQ application can be found in the VANTIQ developer documentation.

### Secure Channels

Communications between clients and the VANTIQ platform occurs over secure channels utilizing SSL. Therefore, communication of credentials to the platform guarantees both the privacy and integrity of the credentials and any response.

## Authorization

VANTIQ offers a full range of controls for authorizing access to application resources. Access controls can be applied to large collections of resources, small collections of resources, or individual resources as dictated by application requirements. An example of fine-grained access control is granting access to an individual object in a VANTIQ application to one or more users. An example of coarse-grained access control is granting access to a collection of objects to one or more users.

Access rights are contained in profiles. A profile specifies a set of resources and the rights granted on each resource identified in the profile. Users are then assigned a profile which associates the rights granted by the profile to the assigned user. Profile assignment is restricted to authorized administrators.

All users and long-lived Access Tokens are assigned a profile and no access to application resources is possible unless it is authorized by the assigned profile.

Profile management and assignment details can be found in the VANTIQ documentation.

# Integrity and Privacy

## Communications

To guarantee the privacy and integrity of data presented to application services, all communications to/from and among VANTIQ hosted services is over encrypted communication links -- either HTTPS or WSS.

This guarantees that the data sent is the data received and that if an intermediary intercepts the message the intermediary cannot read or change the content of the message.

## Application Isolation

VANTIQ Namespaces define an isolated environment for VANTIQ applications. Each namespace guarantees complete separation of the data, situations, recommendations and rules from those of all other namespaces.

VANTIQ operated installations assign namespaces to each VANTIQ customer to enforce isolation of customer applications and data in shared installations. Namespaces may optionally be associated with an organization for purposes of billing and quota management.

The namespace is established at the time the user logs in based on the user's identity. Each authenticated identity is associated with one and only one namespace.

VANTIQ implements namespace data isolation using a traditional “security kernel” architecture that protects all access to data. In VANTIQ’s case this is implemented by qualifying every DML statement with the identity of the namespace. This ensures that requests can only manipulate data that is owned by the specific customer represented by the corresponding namespace.

### Data Encryption

A namespace may be configured with a customer supplied encryption key. This key encrypts the value stored for those VANTIQ type properties defined with the “encrypted” flag. This affords each VANTIQ customer the opportunity to securely store sensitive information using keys available only to that customer.

The encrypted data is decrypted before being returned to a user that is authorized to access the property’s value.

## Edge Devices

### VANTIQ Edge Deployments

Security of a VANTIQ edge installation is dependent on the edge configuration as defined by the customer. Edge devices can only be added to a VANTIQ network by an authorized user.

VANTIQ recommends configuring VANTIQ instances with secure communications (SSL) to protect sensitive information such as access credentials. Each VANTIQ edge device supports the full range of authentication features supported by the cloud implementation. No request will be accepted by any VANTIQ instance unless the caller presents valid credentials. Combined, these capabilities allow edge installations to be as secure as the VANTIQ cloud implementation.

It is important that customers take proper security precautions to avoid additional attack vectors with edge installations such as preventing unauthorized access to the physical edge device and ensuring that the operating systems on the edge devices are configured for security.

### External Sources

Another form of edge device is a Source. A VANTIQ application may create a Source to ingest data from or deliver data to external systems. Not all sources are necessarily secure and security settings for sources are at the discretion of the customer's application development team. For example, a customer may elect to create a less secure source that uses HTTP to access an external service. Alternatively, the customer could choose to use HTTPS to access the external service to guarantee the privacy and integrity of the message traffic.

VANTIQ recommends restricting access to secure endpoints in production applications.

## Audit

### System Audit

VANTIQ automatically maintains a log of security related actions that can be used to audit security related activities.

By default, operations on the following system resources are audited:

- namespaces
- users
- profiles
- nodes
- sources
- tokens

Additional security related events can be audited:

- Authentication using username/ passwords

To serve as an accurate record of actions taken by users, administrators and applications, audits cannot be updated.

### User Audit

Operations on types defined by users will be recorded if the “audited” property on the type definition is set to true. This “audited” flag denotes that all inserts, updates and deletes on that type will record an audit record.

In addition, if more fine-grained auditing is required, users can define their own rules that produce audit entries for specific application activities.

## VANTIQ Operational Security

Cloud hosted VANTIQ operated installations are available in both public and private configurations. VANTIQ utilizes the security features described above to realize security in these VANTIQ operated installations.

### Access Limitations

VANTIQ applies these additional security policies to VANTIQ operated installations to achieve higher levels of privacy and integrity:

- VANTIQ carefully restricts access to cloud hosted infrastructure. Only a very small number of VANTIQ’s most senior and trusted operations staff have access to the raw IaaS resources. This system operator access is primarily for maintenance of the VANTIQ instances and taking backups.
- No VANTIQ employee has access to customer namespaces, including the system operators. Access is restricted to users authorized by the customer that owns the namespace.
- A customer can give a VANTIQ employee access to one of their namespaces, but this is completely at the discretion of the customer.

### IaaS Infrastructure

The IaaS infrastructure hosting instances of VANTIQ are regularly updated with the latest security patches.

## Open Source

VANTIQ maintains an inventory of all open source components used in the product. VANTIQ uses popular and actively developed components so that security vulnerabilities are fixed in a timely fashion. All open source components critical to the security of the VANTIQ infrastructure are updated regularly to the latest version available.