Confidentiality Statement

All parties acknowledge that this document is of a confidential nature and agree, in general, to the confidential nature of any information that is provided by either party to the other, for the preparation of this document and/or for any subsequent contract to be concluded between them, insofar as that information is indicated as being, and/or can reasonably be deemed to be, confidential (hereinafter referred to as Confidential Information).

Neither party may divulge such Confidential Information, orally or in writing, in full or in part, to persons other than their respective employees, representatives, agents or other persons on a need-to-know basis for the performance of this document or any proposal and, more generally, to use this confidential information solely for the purposes of implementing this proposal and agreement.
# Table of Contents

- Confidentiality Statement .................................................................................................................. 2
- Table of Contents ................................................................................................................................. 3
- Overview .................................................................................................................................................. 5
  - 4Deets Communication Infrastructure ............................................................................................... 5
  - Application Security ............................................................................................................................... 5
  - VPN ....................................................................................................................................................... 6
    - VPN User Roles ................................................................................................................................. 6
    - VPN User Management ..................................................................................................................... 6
  - Windows Servers ................................................................................................................................... 6
    - Windows Server User Roles ............................................................................................................... 6
    - User Management ............................................................................................................................. 6
  - Test Automation Server Firewall ......................................................................................................... 7
  - 4Deets Web Application ......................................................................................................................... 7
    - Web Application User Roles .............................................................................................................. 7
    - Project Based Security ....................................................................................................................... 8
    - User Management ............................................................................................................................. 8
  - Database (SQL) ..................................................................................................................................... 8
    - Client/Server Connection .................................................................................................................... 8
    - SQL Server User Roles ...................................................................................................................... 8
    - User Management ............................................................................................................................. 9
# Security Whitepaper

## 4Deets Quality as a Service (QaaS)

---

### Approval for use

<table>
<thead>
<tr>
<th>Exaserv</th>
<th>Name</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setup by:</td>
<td>Kyung Kim</td>
<td></td>
<td>June 15&lt;sup&gt;th&lt;/sup&gt; 2018</td>
</tr>
<tr>
<td>Approved by:</td>
<td>Wim De Smet</td>
<td></td>
<td>June 21&lt;sup&gt;st&lt;/sup&gt; 2018</td>
</tr>
</tbody>
</table>

### Distribution

---

### Change History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>June 21&lt;sup&gt;st&lt;/sup&gt; 2018</td>
<td>Final version</td>
</tr>
</tbody>
</table>

---

© 2018 4Deets
Security Whitepaper – 4Deets Quality as a Service (QaaS)
Overview

4Deets Communication Infrastructure

Application Security

4Deets ensures data and application security by using the following technologies:

- Firewall – firewall ensures that only the allowed connections are made to and from the 4Deets testing server
  - HTTPS inbound call to port 443 for 4Deets web accesses (Jenkins web server)
  - HTTPS outbound call to SuccessFactors servers
  - HTTPS outbound call to SAP Hana Cloud Platform GIT server
- VPN connection using RDP (port 3389) by authenticated 4Deets developers only
- SSL data encryption – data traffics are encrypted via SSL encryption (HPPTS and TLS VPN)
VPN

VPN with TLS protocol is used for all RDP (Remote Desktop Protocol) connections to the 4Deets development environment. Except for the HTTPS call to the 4Deets web accesses, only the RDP connections via the VPN are open. Only the 4Deets developers are given accesses through the VPN. Customers are not given accesses via the VPN.

The following resources are available via the VPN:

- 4Deets Test Automation servers (production and sandbox)
- Database tables running on SQL (test user profiles, system configurations, and test data)

VPN User Roles

The following user roles are defined in 4Deets VPN:

- Super User – admin with all rights
- Developers – accesses 4Deets development resources (Windows Servers and SQL)

VPN User Management

User ID’s are assigned to a new developer upon an approval of developer accesses by 4Deets CTO.

User ID’s are purged together with all accesses to 4Deets systems upon a user leaving the 4Deets developer role.

Windows Servers

Windows Server User Roles

The following user roles are defined in 4Deets Windows Servers:

- Super User – admin with all rights
- Developers – limited admin rights and full development accesses

User Management

User ID’s are assigned to a new developer upon an approval of developer accesses by 4Deets CTO.

User ID’s are purged together with all accesses to 4Deets systems upon a user leaving the 4Deets developer role.
Test Automation Server Firewall

Allowed Inbound Calls:

- HTTPS call to port 443 from anywhere
- RDP connections to port 3389 via TLS VPN only

Allowed Outbound Calls:

- HTTPS requests by web browsers Internet Explorer, Edge, Chrome, and Firefox to the following sites:
  - SuccessFactors cloud application servers
  - SuccessFactors provisioning servers
  - SAP Hana Cloud GIT
  - 4Deets web services (prod and snd)

4Deets Web Application

Only 4Deets Web Application is exposed via the HTTPS port (443). No other services are available via HTTPS. HTTP port (80) is closed.

Web Application User Roles

The following user roles are defined in 4Deets Web Application:

- Super User – admin with all rights
- Developers – developer roles with limited admin rights and ability to run all jobs
- Customer users – access customer-specific folders only; cannot run jobs

<table>
<thead>
<tr>
<th>Roles</th>
<th>Super User</th>
<th>Developer</th>
<th>Customer User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Rights</td>
<td>All</td>
<td>Limited</td>
<td>None</td>
</tr>
<tr>
<td>User Admin</td>
<td>All</td>
<td>Limited</td>
<td>None</td>
</tr>
<tr>
<td>Test Projects</td>
<td>All</td>
<td>All</td>
<td>Own Project</td>
</tr>
<tr>
<td>Test Executions</td>
<td>Edit/Run/View</td>
<td>Edit/Run/View</td>
<td>View only</td>
</tr>
<tr>
<td>Test Data</td>
<td>Edit/View</td>
<td>Edit/View</td>
<td>Edit/View</td>
</tr>
<tr>
<td>Views</td>
<td>Edit/View</td>
<td>Edit/View</td>
<td>Edit/View</td>
</tr>
<tr>
<td>Reports</td>
<td>View</td>
<td>View</td>
<td>View</td>
</tr>
</tbody>
</table>
Project Based Security

All test scenarios are managed by Projects and Sub-projects. Each project is specific to a single customer. All customer users are restricted to view only the projects specific to the customer account.

User Management

Developer Users

- Developer User ID’s are assigned to a new developer upon an approval of developer accesses by 4Deets CTO.
- Developer User ID’s are purged together with all accesses to 4Deets systems upon a user leaving the 4Deets developer role.

Customer Users

- Customer User ID’s are created upon onboarding a new customer to 4Deets services or when a new customer user is requested by a trusted contact in the customer organization
- A Customer User ID is removed (deleted) from the 4Deets Test Automation server upon termination of 4Deets services or upon request by a trusted contact in the customer organization

Database (SQL)

Client/Server Connection

Connection from 4Deets Test Automation servers to SQL uses SQL Connector and the entire data exchange remains within the VPN. The SQL Connector has whitelisted the IP addresses of the 4Deets Test Automation servers. Only the requests from the whitelisted IP address are accepted.

SQL Server User Roles

The following user roles are defined in 4Deets Windows Servers:
• Developer User – admin with all rights

User Management

User ID’s are assigned to a new developer upon an approval of developer accesses by 4Deets CTO.

User ID’s are purged together with all accesses to 4Deets systems upon a user leaving the 4Deets developer role.