Oracle® Hospitality Suite8

Security Guide
Release 8.10.0.0
Part Number: E69616-01

May 2016

ORACLE

Contents

Preface

This document provides security reference and guidance for Suite8.

Audience

This document is intended for:

- System administrators installing Suite8.
- End users of Suite8.

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:

https://support.oracle.com

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received
- Screen shots of each step you take

Documentation

Oracle Hospitality product documentation is available on the Oracle Help Center at http://docs.oracle.com/en/industries/hospitality/

Related Documentation

PCI Security Standards Council Reference Documents

The following documents provide additional detail surrounding the PCI SSC and related security programs (PA-DSS, PCI DSS, and so forth.):

- Payment Card Industry Payment Applications - Data Security Standard (PCI PA-DSS)
- Payment Card Industry Data Security Standard (PCI DSS)
- Center for Internet Security (CIS) Benchmarks (used for OS Hardening)

Guides and Best Practices:

- Suite8 Install Shield_8100
- Suite8 Property - PA-DSS Data Security Standard Implementation Guide - Version 8.10.0.0
- Suite8 Homepage
- How to Install SSL

Revision History

Date	Description of Change
May, 2016	• Initial publication.

1 Suite8 Security Overview

This chapter provides an overview of Oracle Hospitality Suite8 security and explains the general principles of application security.

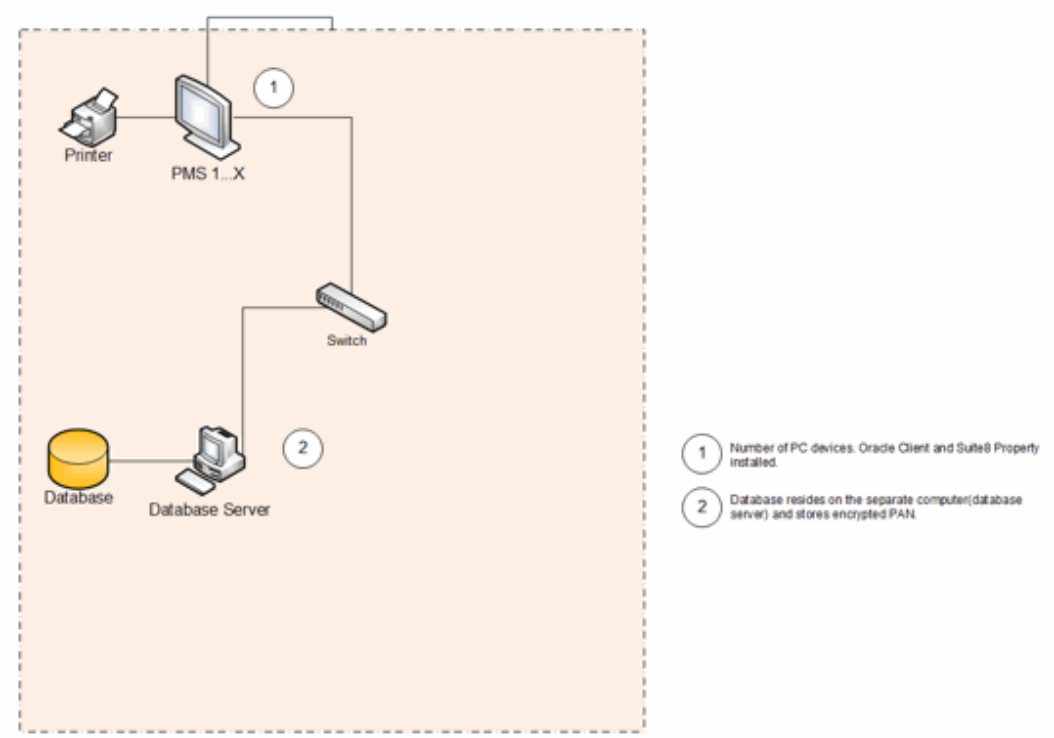
Basic Security Considerations

The following principles are fundamental to using any application securely:

- **Keep software up to date.** This includes the latest product release and any patches that apply to it.
- **Limit privileges as much as possible.** Users should be given only the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
- **Monitor system activity.** Establish who should access which system components, and how often, and monitor those components.
- **Install software securely.** For example, use firewalls, secure protocols using TLS (SSL), and secure passwords. See "Performing a Secure Suite8 Installation" for more information.
- **Learn about and use the Suite8 security features.** See "Implementing Suite8 Security" for more information.
- **Use secure development practices.** For example, take advantage of existing database security functionality instead of creating your own application security. See "Security Considerations for Developers" for more information.
- **Keep up to date on security information.** Oracle regularly issues security-related patch updates and security alerts. You must install all security patches as soon as possible. See the Critical Patch Updates and Security Alerts Web site:

Overview of Suite8 Security

Figure 1-1 Suite8 Property Network Diagram without Credit Card Interface



In accordance with the PA DSS Data Security Standard, Oracle strongly recommends that every site installs and maintains a firewall configuration to protect data. Configure your network so that databases and client PCs always reside behind a firewall and have no direct access to the Internet.

Oracle strongly recommends that each site ensures that servers, databases, client PCs, and any medium containing sensitive data reside behind a firewall.

Firewalls are computer devices that control the computer traffic allowed into a company's network from outside, as well as traffic into more sensitive areas within a company's internal network. All systems need to be protected from unauthorized access from the Internet, whether for e-commerce, employees' Internet-based access via desktop browsers, or employees' email access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

Understanding the Suite8 Environment

When planning your Suite8 implementation, consider the following:

- **Which resources need to be protected?**
  - You need to protect customer data, such as credit-card numbers.
  - You need to protect internal data, such as proprietary source code.
  - You need to protect access data to third party interfaces from misuse.
  - You need to protect system components from being disabled by external attacks or intentional system overloads.

- **Who are you protecting data from?** For example, you need to protect your subscribers' data from other subscribers, but someone in your organization might need to access that data to manage it. You can analyze your workflows to determine who needs access to the data; for example, it is possible that a system administrator can manage your system components without needing to access the system data.
- **What will happen if protections on strategic resources fail?** In some cases, a fault in your security scheme is nothing more than an inconvenience. In other cases, a fault might cause great damage to you or your customers. Understanding the security ramifications of each resource will help you protect it properly.

Oracle provides functionality within the Suite8 Application for Personal Information (for example, passport, date of birth, and credit card). Placing this information in any fields other than the designated areas, i.e., Notes or Comments fields, is open for PCI review and is not compliant with PA-DSS rules and regulations.

Recommended Deployment Configurations

This section describes recommended deployment configurations for Suite8.

There are different deployment scenarios possible depending on the used dataflow and installed interfaces.

Credit/Debit Cardholder Dataflow Diagram

Figure 1-2 Suite8 without CC Interface

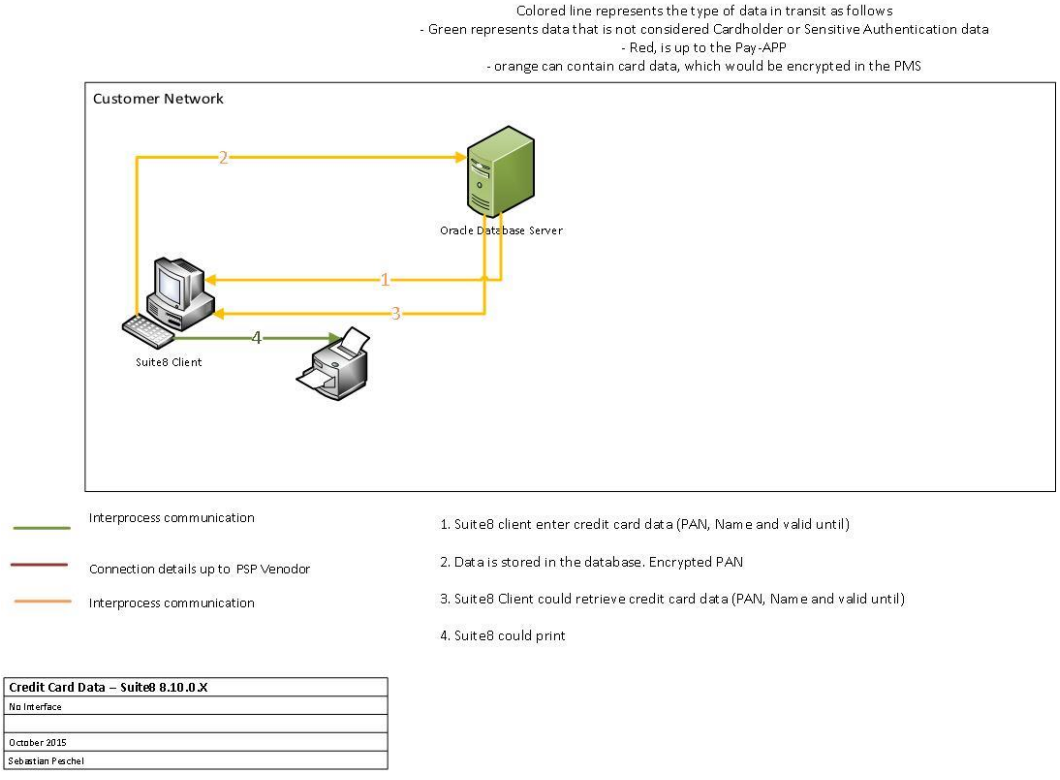
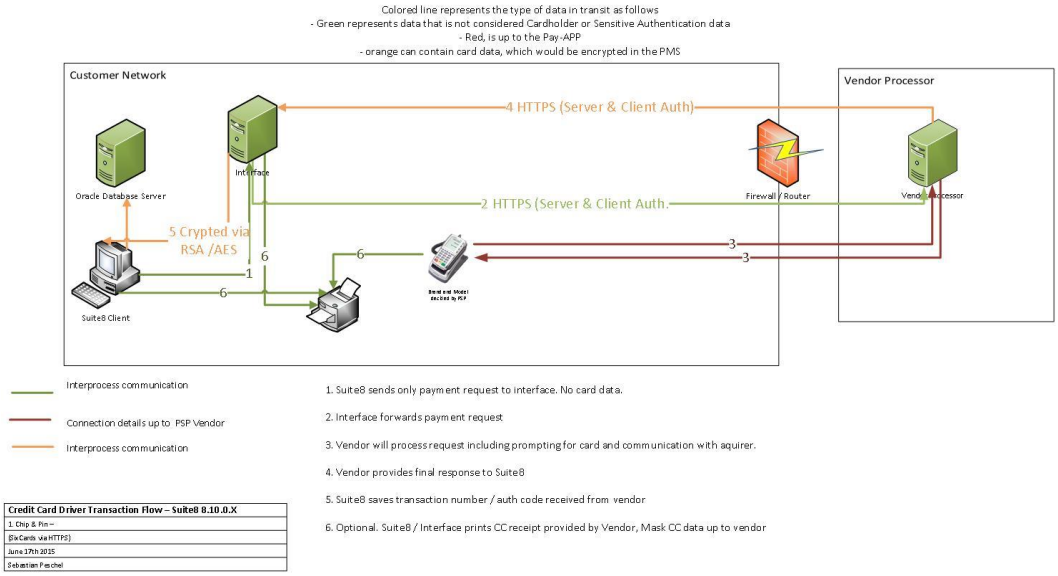
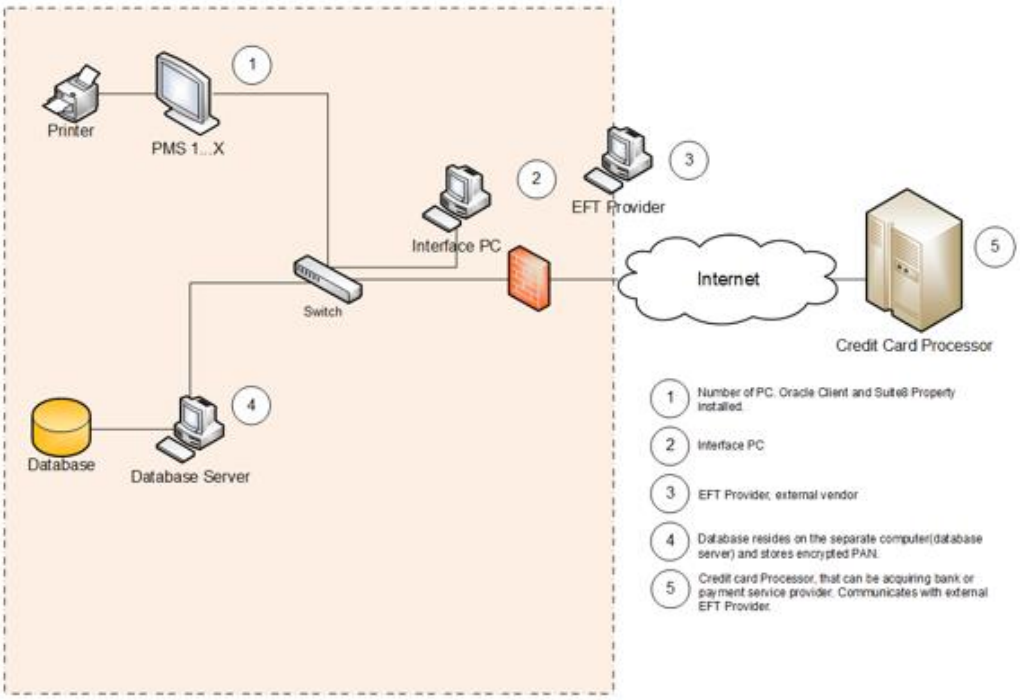


Figure 1-3 Suite8 Chip & Pin HTTPS



The following picture shows an example of the deployment diagram when a Chip & Pin interface is used:

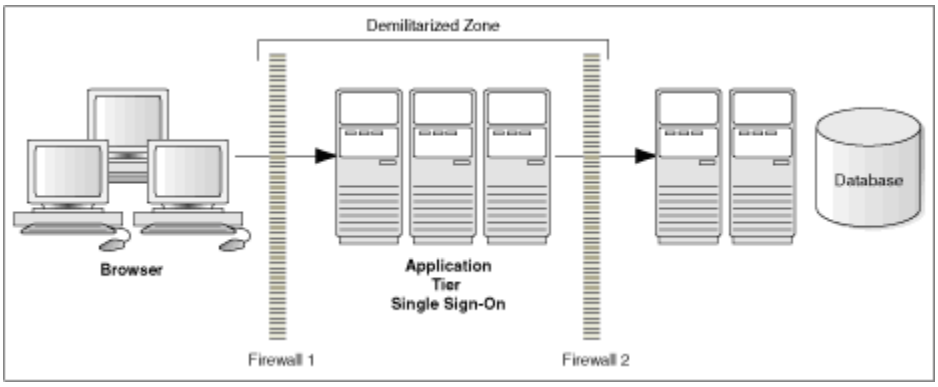
Figure 1-4 Suite8 Property Network Diagram with Credit Card Interface



For more options see the latest "Suite8 Property - PA-DSS Data Security Standard Implementation Guide for Suite8".

The general architectural recommendation is to use the well-known and generally accepted Internet-Firewall-DMZ-Firewall-Intranet architecture shown in Figure 1-5.

Figure 1-5 Traditional DMZ View



The term demilitarized zone (DMZ) refers to a server that is isolated by firewalls from both the Internet and the intranet, thus forming a buffer between the two. Firewalls separating DMZ zones provide two essential functions:

- Blocking any traffic types that are known to be illegal
- Providing intrusion containment, should successful intrusions take over processes or processors

Component Security

Operating System Security

See the Network Security Checklists.

Oracle Database Security

See the Oracle Database Security Guide for 11.2.

Internet Information Server Security

In case IIS based interfaces are used, refer to Security Guidance for IIS.

2 Performing a Secure Suite8 Installation

This chapter presents planning information for your Suite8 installation. For information about installing Suite8, see the Suite8 Installation Guide.

The 12 Requirements of the PCI DSS

Build and Maintain a Secure Network and Systems

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data

3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.

Maintain a Vulnerability Management Program

5. Protect all systems against malware and regularly update anti-virus software or programs.
6. Develop and maintain secure systems and applications.

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need-to-know.
8. Identify and authenticate access to system components.
9. Restrict physical access to cardholder data.

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.

Maintain an Information Security Policy

12. Maintain a policy that addresses information security for all personnel. See the latest Suite8 Property - PA-DSS Data Security Standard Implementation Guide. This chapter presents planning information for your Suite8 installation.

For information about installing Suite8, see Suite8 Installation Guide.

Pre-Installation Configuration

Install and maintain a firewall configuration to protect data.

Do not use vendor-supplied defaults for system passwords and other security parameters.

Hackers (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and easily determined via public information.

Suite 8 does not provide default accounts.

Installing Suite8 Securely

The following guides are a pre-requisite before installing Suite8:

- Suite8 Install Shield_8100
- Suite8 Property - PA-DSS Data Security Standard Implementation Guide - Version 8.10.0.0
- Suite8 Homepage
- How to Install SSL

These Guides and Best Practices can be found on the Oracle Help Center.

You can perform a custom installation or a typical installation. Perform a custom installation to avoid installing options and products you do not need. If you perform a typical installation, remove or disable features that you do not need after the installation.

When installing the DB, you are obliged to create secure DB passwords. Do not use default or well-known passwords and rotate passwords frequently.

See the "Oracle Hospitality Suite8 Installation Guide" for more information and instructions.

Installing Suite 8 Spa and Leisure Subcomponent Securely

The following guides are a pre-requisite before installing Suite8 Spa and Leisure

- Suite8 Spa and Leisure Install Shield_8100
  (Installation Guide for Suite8 Leisure_8.10.0.0)
- Installation of the Web Services via SSL using URL Rewriting

Post-Installation Configuration

- Remove or disable components that are not needed in a given type of deployment.
- Configure communications security. In case WebConnect or XML Interface is used SSL must be installed on the IIS server. See "How to Install SSL" document for more details. Weak or plain-text protocols, such as FTP, must be disabled. It is still possible to enable them for backward compatibility (or communication with third parties which still don't support secure protocols), however this might be insecure. It is planned for the future versions to completely disable insecure protocols.
- Enable User Access Control.
- Change the User Access Rights for the Oracle Client/Suite8 Client files to be restrictive (See Suite8 Install Shield_8100 for the details).
- Enable User Log for all sensitive data.
- When possible, access to XML Interface has to be restricted using firewall rules to allow requests only from the trusted IP addresses. For example when only WebConnect is used, firewall has to be configured to allow only the traffic from the know WebConnect Web Server.

Change Default Passwords

Suite8 is not installed with any default passwords.

When defining the passwords, use Complex Passwords and change them frequently.

Supervisor or members of the Supervisor Group are not to be used by regular users and must only be used by authorized Administrators.

3 Implementing Suite8 Security

This chapter explains the Suite8 security features. Suite 8 provides 2 options for user authentication:

- Suite 8 native authentication

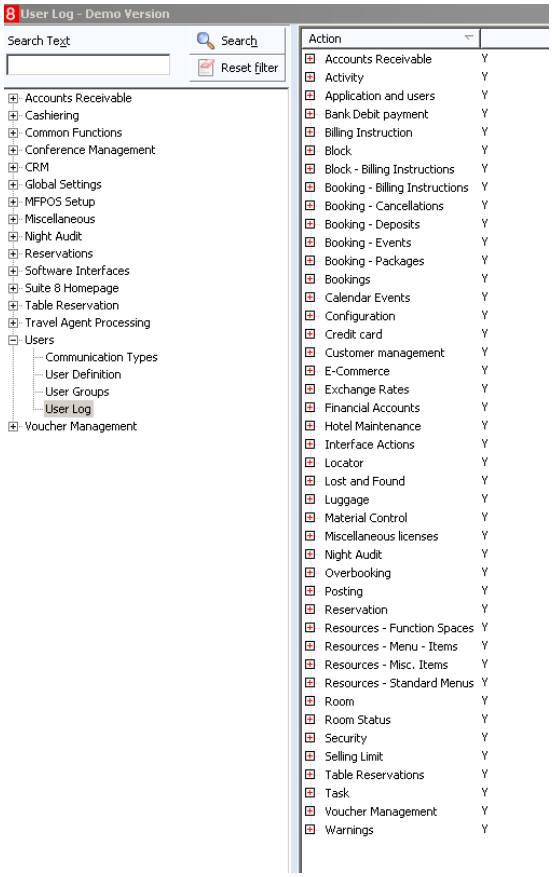
  In this case all user management and password control mechanisms are implemented by Suite 8. Access Controls definition and password rules are done in Suite 8.

  In order to comply with PA DSS rules, you must set:

  - Password requirements to have a minimum of 7 characters and include both numeric and alphabetic characters
  - Password change requirements to be at least every 90 days
  - Password history management to require new passwords to not repeat the previous four passwords.
  - Repeated access attempts to lock out the user account after a maximum of six logon attempts
  - Lockout duration to a minimum of 30 minutes or until an administrator enables the user ID
  - Re-authentication requirements to re-activate the session if the application session has been idle for more than 15 minutes
- LDAP authentication. The property can decide to use existing LDAP server (e.g. Microsoft Exchange server). In this case user configuration and password management is managed by the LDAP Server.

Make sure the property has logging turned on and configured in accordance with PCI DSS 10.2 and 10.3 as follows:

1. Navigate to Setup -> Configuration -> Users -> User Log.
2. Set all logs to **yes**.



The format of the log file is not configurable and always stores the following information:

- User identification
- Type of event
- Date and time
- Action indication
- Origination
- Name and component or resources

Implement automated assessment trails for all system components to reconstruct the following events:

1. All individual user accesses to cardholder data from the application
2. All actions taken by any individual with administrative privileges in the application
3. Access to application audit trails managed by or within the application
4. Invalid logical access attempts
5. Use of the application's identification and authentication mechanisms (including but not limited to creation of new accounts, elevation of privileges, etc.) and all changes, additions, deletions to application accounts with root or administrative privileges
6. Initialization, stopping, or pausing of the application audit logs
7. Creation and deletion of system-level objects within or by the application

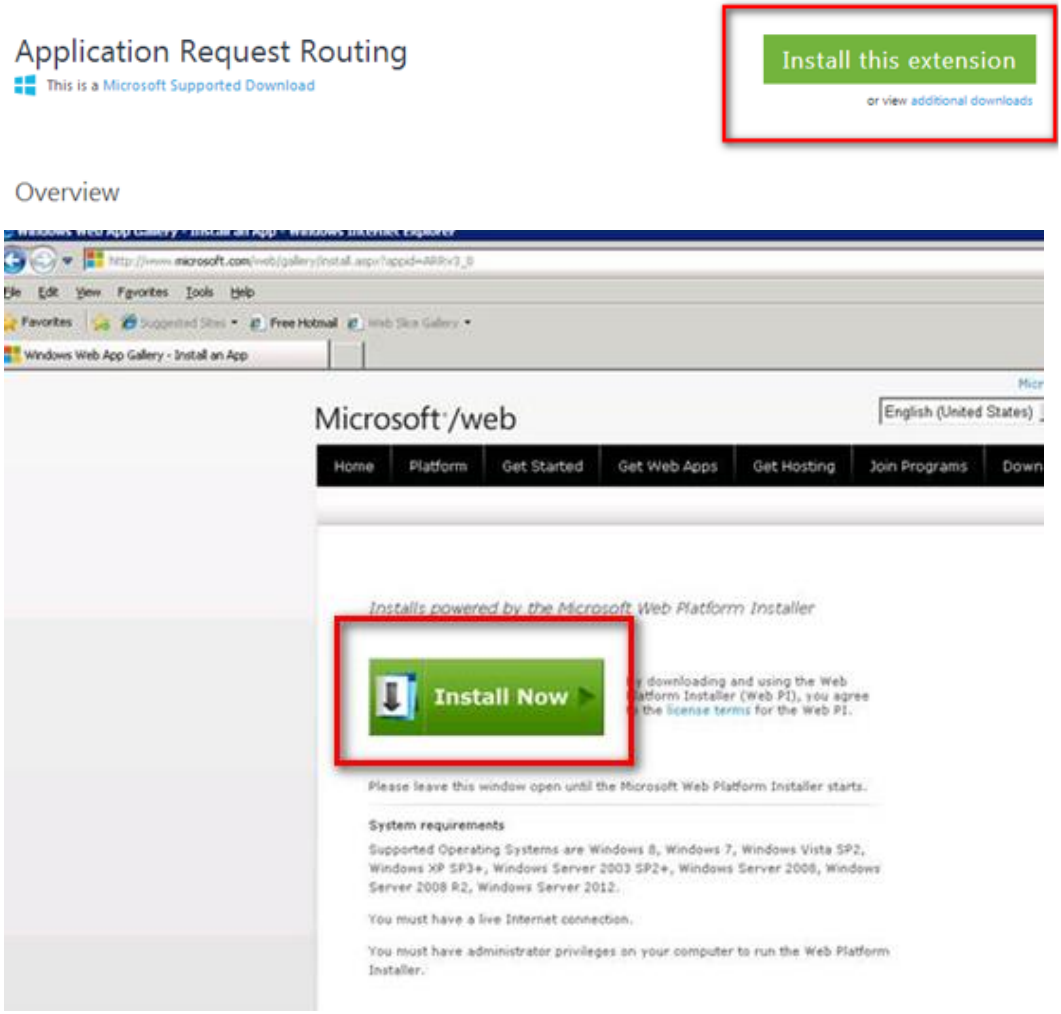
Record at least the following assessment trail entries for all system components for each event from 10.2.x above:

1. User identification
2. Type of event
3. Date and time
4. Success or failure indication
5. Origination of event
6. Identity or name of affected data, system component, or resource.

Disabling or subverting the logging function of Suite8 Property in any way will result in non-compliance with PCI DSS.

4 Installation of the Web Services via SSL using URL Rewriting

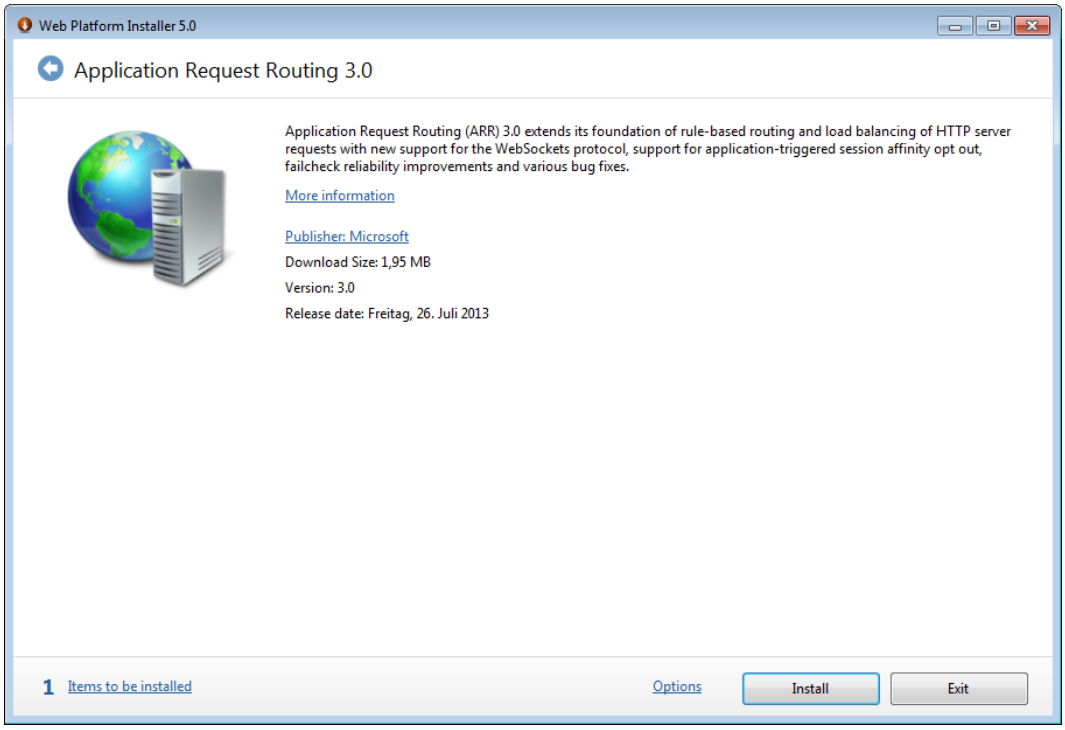
1. Install Application Request Routing (ARR) from
   http://www.iis.net/downloads/microsoft/application-request-routing
   It can be either done by using Web Platform Installer
   Click **Install this Extension.**



   or

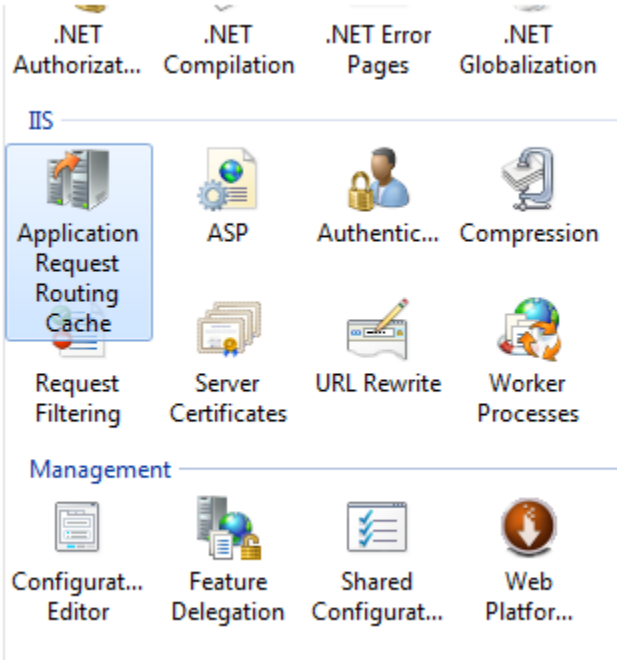
   By downloading the installer directly from
   http://www.iis.net/downloads/microsoft/application-request-routing#additionalDownloads

2. Follow the on screen instructions..

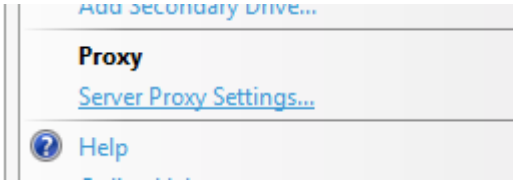


Now that the Application Request Routing (ARR) module has been installed we need to configure it to act as a proxy server (this functionality isn't enabled by default).

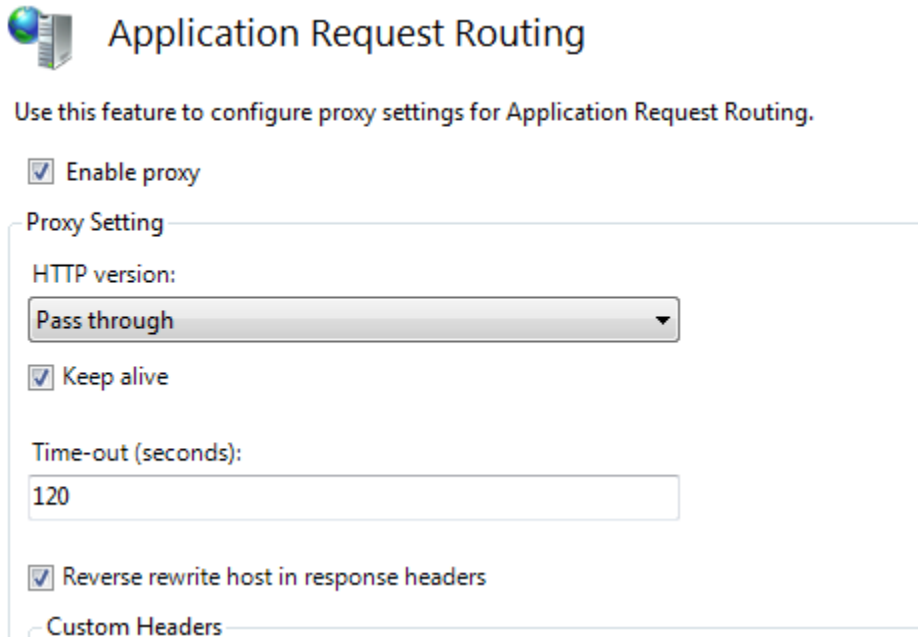
3. Launch **Internet Information Server (IIS) Management**.
4. In IIS Manager highlight the Application Request Routing Cache feature and click **Open Feature** in the Actions pane.



5. Click **Server Proxy Settings** in the Actions pane.

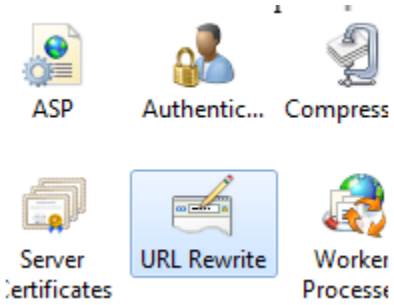


6. Tick the **Enable proxy** checkbox and then click **Apply**. Leave all the default values in place.

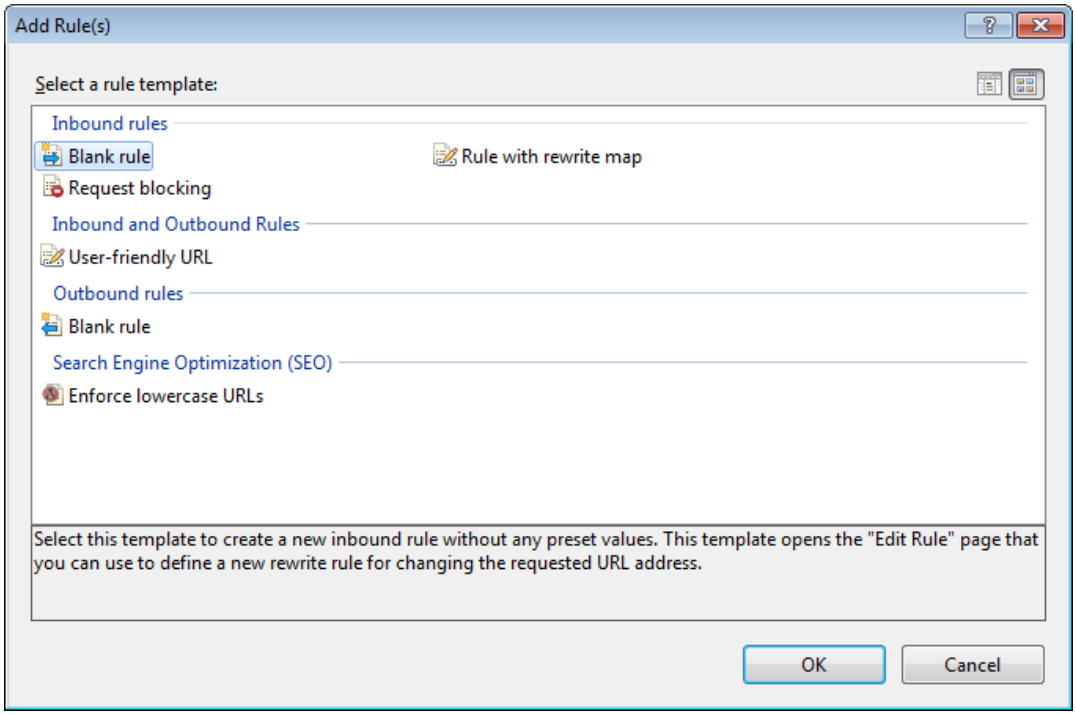


Next we need to configure a URL Rewrite rule so that IIS knows what to do with requests which we want to forward to Tomcat.

7. Click the **Default Web Site**, highlight the **URL Rewrite** icon and then click **Open Feature** in the Actions pane.

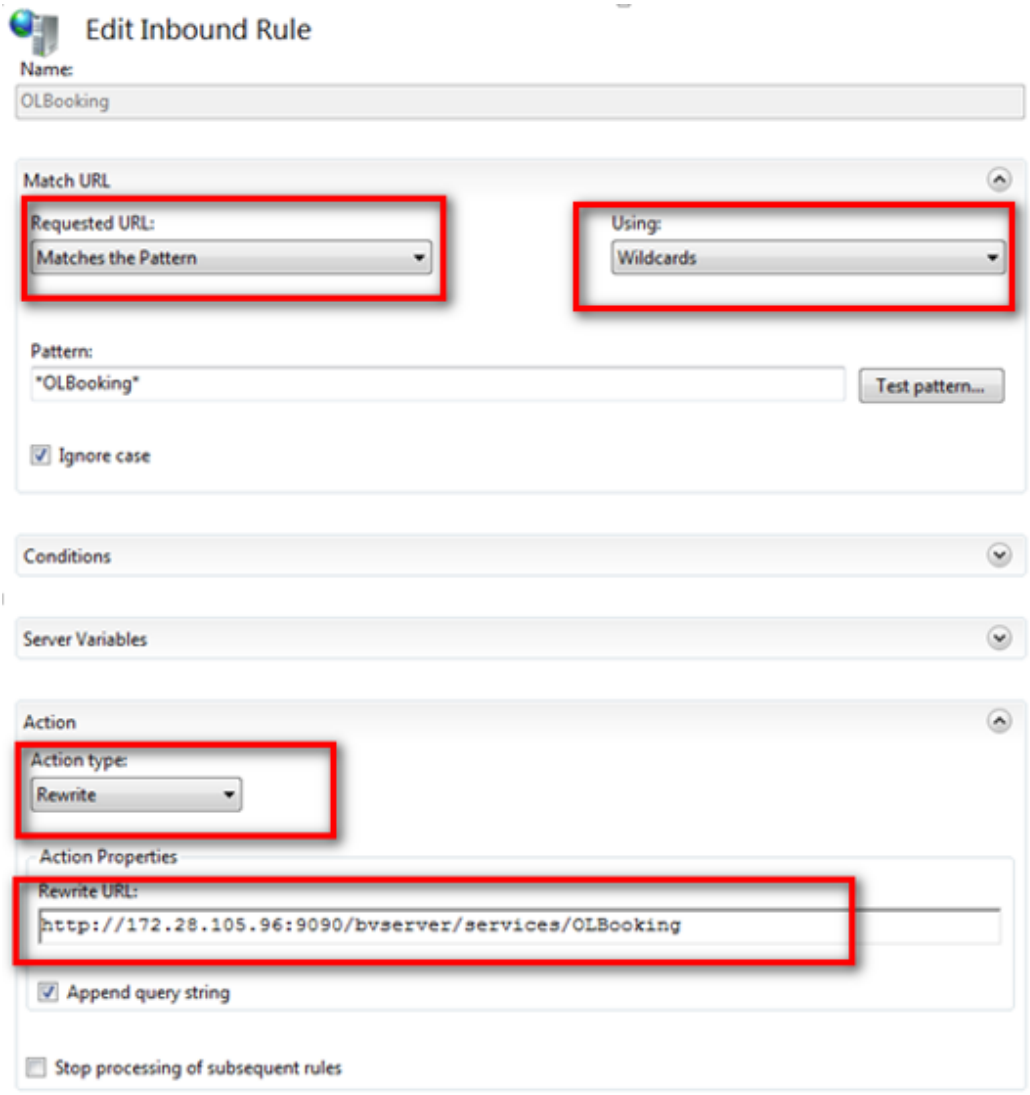


8. In the URL Rewrite feature click **Add Rules** in the Actions Pane.
9. In the Add Rule(s) dialog box select **Blank rule** and click **OK**.



10. In the Edit Inbound Rule feature assign a name to the new rule in the Pattern dialog box.
11. In the *Match URL* group select following values:
    * Requested URL – Matches the Pattern
    * Using – Wildcards
    * Pattern – How to recognise the URL (in case of Bellavita it can be for example ***OLBooking***)
12. In the *Action* group select following values:
    * Action Type – Rewrite
    * Rewrite URL – Here you have to write the URL of the working server (e.g. Bellavita Web Service URL)

    The new rule should default to using Regular Expressions (if it doesn't ensure that you select this option)



13. If everything is configured properly – directing your browser to the URL http://SERVERNAME/OLBooking the response of the URL specified in the "Rewrite URL" will be returned.

Appendix A Secure Deployment Checklist

The following security checklist includes guidelines that help secure your database:

- Install only what is required.
- Lock and expire default user accounts.
- Enforce password management.
- Enable data dictionary protection.
- Practice the principle of least privilege.
    - Grant necessary privileges only.
    - Revoke unnecessary privileges from the PUBLIC user group.
    - Restrict permissions on run-time facilities.
- Enforce access controls effectively and authenticate clients stringently.
- Restrict network access.
- Apply all security patches and workarounds.
    - Use a firewall.
    - Never poke a hole through a firewall.
    - Protect the Oracle listener.
    - Monitor listener activity.
    - Monitor who accesses your systems.
    - Check network IP addresses.
    - Encrypt network traffic.
    - Harden the operating system.