

ПК «SafeERP Security Suite»
Установка, удаление

Аннотация

Данное руководство является программным документом, определяющим порядок установки и удаления компонентов программного комплекса (далее – ПК) «SafeERP Security Suite». Руководство содержит сведения, необходимые для обеспечения взаимодействия системного программиста (администратора) ПК «SafeERP Security Suite» с программным обеспечением ПК на своем автоматизированном рабочем месте. Настоящее руководство состоит из информационной части (аннотации и листа содержания) и разделов основной части, включающих в себя:

- сведения о назначении ПК «SafeERP Security Suite»;
- условия работы ПК «SafeERP Security Suite»;
- порядок установки ПК «SafeERP Security Suite»;
- порядок удаления компонентов ПК «SafeERP Security Suite»;
- сообщения системному программисту.

Содержание

1. Назначение ПК «SafeERP Security Suite»	5
2. Условия работы ПК «SafeERP Security Suite»	6
2.1. Компоненты ПК «SafeERP Security Suite»	6
2.2. Технические средства, обеспечивающие работу ПК «SafeERP Security Suite»	6
2.3. Программные средства, обеспечивающие работу ПК SafeERP	7
3. Установка агентов ПК «SafeERP Security Suite»	8
3.1. Установка ПК агентов	8
3.1.1. Установка ABAP-агента	8
3.1.2. Установка Java-агента	13
3.1.3. Установка BO-агента	21
3.1.4. Установка HANA-агента	23
3.2. Создание системных УЗ агентов ПК «SafeERP Security Suite»	26
3.2.1. Создание пользователя на ABAP-агенте	26
3.2.2. Создание пользователя на Java-агенте	26
3.2.3. Создание пользователя на BO-агенте	28
3.2.4. Создание пользователя на HANA-агенте	31
3.3. Установка сервера управления ПК «SafeERP Security Suite»	32
3.3.1. Активация BC Set	33
3.3.2. Настройка компонента SAP FIORI	33
3.3.3. Активация сервисов	34
3.3.4. Настройка RFC-групп	34
3.3.5. Активация SAP Gateway	34
3.3.6. Создание пользователя с правами оператора ПК «SafeERP Security Suite»	36
3.3.7. Создание пользователя с правами администратора ПК «SafeERP Security Suite»	38
3.3.8. Создание RFC-соединения от сервера управления к ABAP-агенту	38
3.3.9. Создание RFC-соединения от сервера управления к Java-агенту	40
3.3.10. Создание RFC-соединения от сервера управления к BO-агенту	42
3.3.11. Создание RFC-соединения от сервера управления к HANA-агенту	44
3.4. Включение ПК «SafeERP Security Suite » в транспортную систему агента	46
3.5. Включение ПК «SafeERP Security Suite» в систему проверки кода	52
4. Удаление ПК «SafeERP Security Suite»	55

4.1.	Удаление ПК «SafeERP Security Suite »	55
4.2.	Удаление компонентов ПК «SafeERP Security Suite»	57
4.2.1.	Удаление RFC-соединений	57
4.2.2.	Удаление учетных записей	57
4.2.3.	Удаление ABAP-агента	58
4.2.4.	Удаление Java-агента	59
4.2.5.	Удаление BO-агента	60
4.2.6.	Удаление HANA-агента	61
5.	Сообщения системному программисту	64

1. Назначение ПК «SafeERP Security Suite»

ПК «SafeERP Security Suite» предназначен для контроля (анализа) защищенности и контроля целостности информационно-программных ресурсов многопользовательских автоматизированных систем на базе прикладного программного обеспечения производства компании SAP. ПК «SafeERP Security Suite» функционирует в интеграционной платформе SAP NetWeaver.

Областью контроля ПК «SafeERP Security Suite» являются:

- программные объекты SAP-системы;
- настройки программного обеспечения и средств защиты SAP-системы;
- программный код ABAP.

ПК «SafeERP Security Suite» выявляет:

- изменение целостности программных объектов;
- уязвимости в настройке программного обеспечения и средствах защиты;
- недостатки (ошибки) программного кода ABAP прикладного программного обеспечения.

2. Условия работы ПК «SafeERP Security Suite»

2.1. Компоненты ПК «SafeERP Security Suite»

ПК «SafeERP Security Suite» состоит из следующих компонентов:

- сервер управления ПК;
- ABAP-агент ПК (агент для систем SAP NetWeaver на ABAP-стеке);
- Java-агент ПК (агент для систем SAP NetWeaver на Java стеке);
- BO-агент ПК (агент для систем SAP Business Objects);
- HANA-агент ПК (агент для систем SAP HANA).

Общая схема работы ПК представлена на рис. 1.

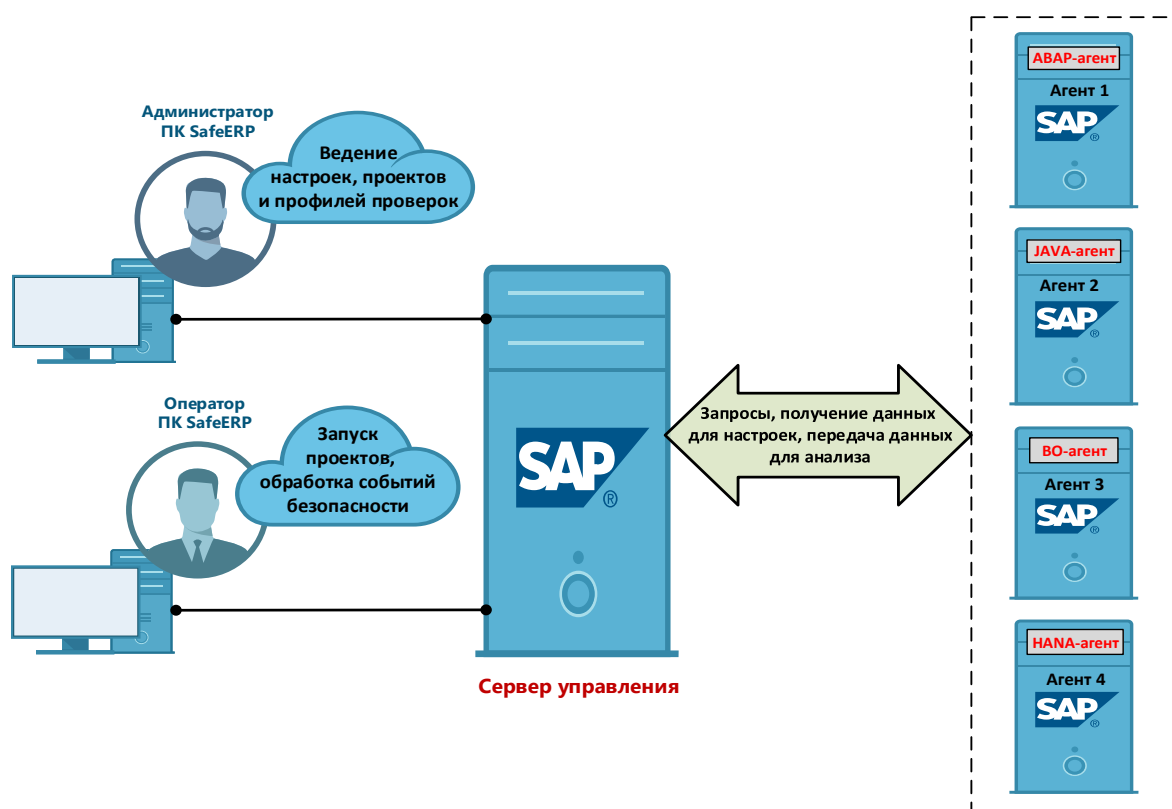


Рисунок 1 – Общая схема работы ПК «SafeERP Security Suite»

2.2. Технические средства, обеспечивающие работу ПК «SafeERP Security Suite»

К техническим средствам, обеспечивающим работу ПК, относятся: сервер управления, автоматизированные рабочие места оператора и администратора ПК «SafeERP Security Suite». Дополнительных требований к техническим средствам при установке ПК не предъявляется. ПК «SafeERP Security Suite» может быть установлен на любом техническом средстве заказчика, где уже установлена система SAP и составляющие ее компоненты.

2.3. Программные средства, обеспечивающие работу ПК SafeERP

Программное обеспечение ПК «SafeERP Security Suite» состоит из серверной части и агентской части. Серверная часть устанавливается на SAP-систему, где будет работать оператор ПК «SafeERP Security Suite». Серверная часть содержит функционал для анализа объектов SAP-системы на безопасность. Для получения данных о проверяемом объекте серверная часть посылает запрос агентской части. Агентская часть устанавливается на SAP-систему, объекты которой необходимо анализировать. Агентская часть содержит набор функций, которые по запросу собирают данные о проверяемом объекте и передают их на серверную часть для анализа. Программное обеспечение ПК позволяет осуществлять прямое обращение к коду системы SAP без выгрузки кода.

Для работы сервера управления необходимо следующее:

- платформа SAP NetWeaver AS ABAP не ниже версии 7.52 с установленным компонентом SAP FIORI FRONT-END SERVER не ниже версии 6.0 и компонентом SAP_UI 7.54.

Примечание. Допускается некорректная работа ПК «SafeERP Security Suite» в интерфейсе SAP FIORI на версиях SAP_UI ниже 7.54 SP05, а также на SAP_UI 7.54 с более ранними пакетами поддержки, в том числе SP04 и ниже.

Для работы агентов необходимы платформы:

- для ABAP-агента – SAP NetWeaver AS ABAP не ниже версии 7.0;
- для Java-агента – SAP NetWeaver AS Java не ниже версии 7.31;
- для BO-агента – SAP BusinessObject BI не ниже версии 4.1;
- для HANA-агента – SAP HANA не ниже версии 1.0.

На автоматизированные рабочие места оператора и администратора ПК «SafeERP Security Suite» должны быть установлены: SAP GUI for Windows не ниже версии 7.50 и Microsoft Office – для формирования и просмотра отчетов.

3. Установка агентов ПК «SafeERP Security Suite»

3.1. Установка ПК агентов

3.1.1. Установка АВАР-агента

Для установки агента на систему необходимо зайти в SAP-систему агента ПК «SafeERP Security Suite» (в мандант системы 000) под учетной записью администратора системы с правами на установку пакетов и работу с пользователями, запустить транзакцию SAINT и выполнить действия в следующей последовательности:

- 1) Выбрать пункт меню «Installation package» -> «Load packages» -> «From frontend».
- 2) Выбрать файл «AA_NNN_nnn_type.SAR» в директории на установочном диске \Installation\Agent, где NNN – обозначение версии платформы, nnn – номер версии.
- 3) Нажать кнопку «Открыть» (рис. 2).



Рисунок 2 – Выбор файла пакета инсталляции

- 4) В появившемся окне нажать кнопку «Decompress» (рис. 3).
Примечание. При наличии недеблокированных транспортных запросов в системе, их необходимо пропустить при установке.

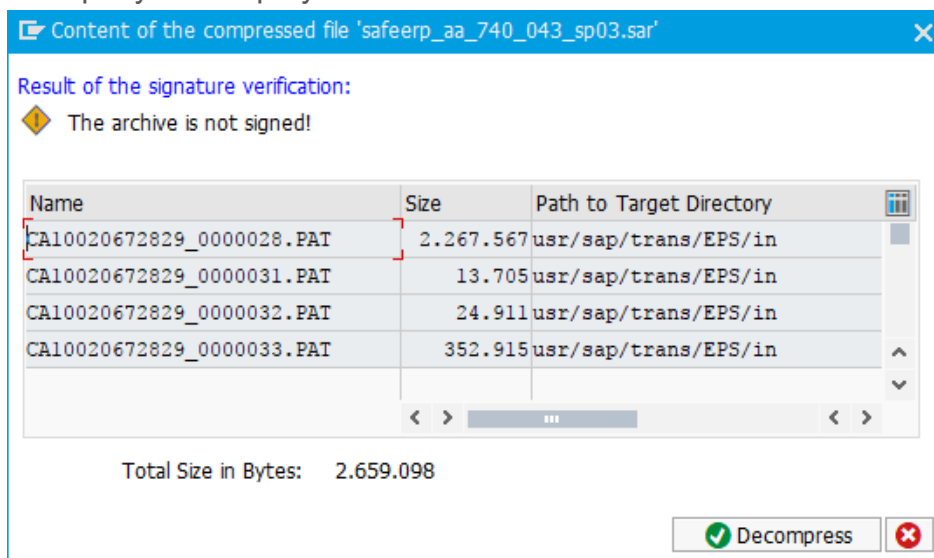


Рисунок 3 – Распаковка установочного файла

- 5) Нажать кнопку «Start» (рис. 4).

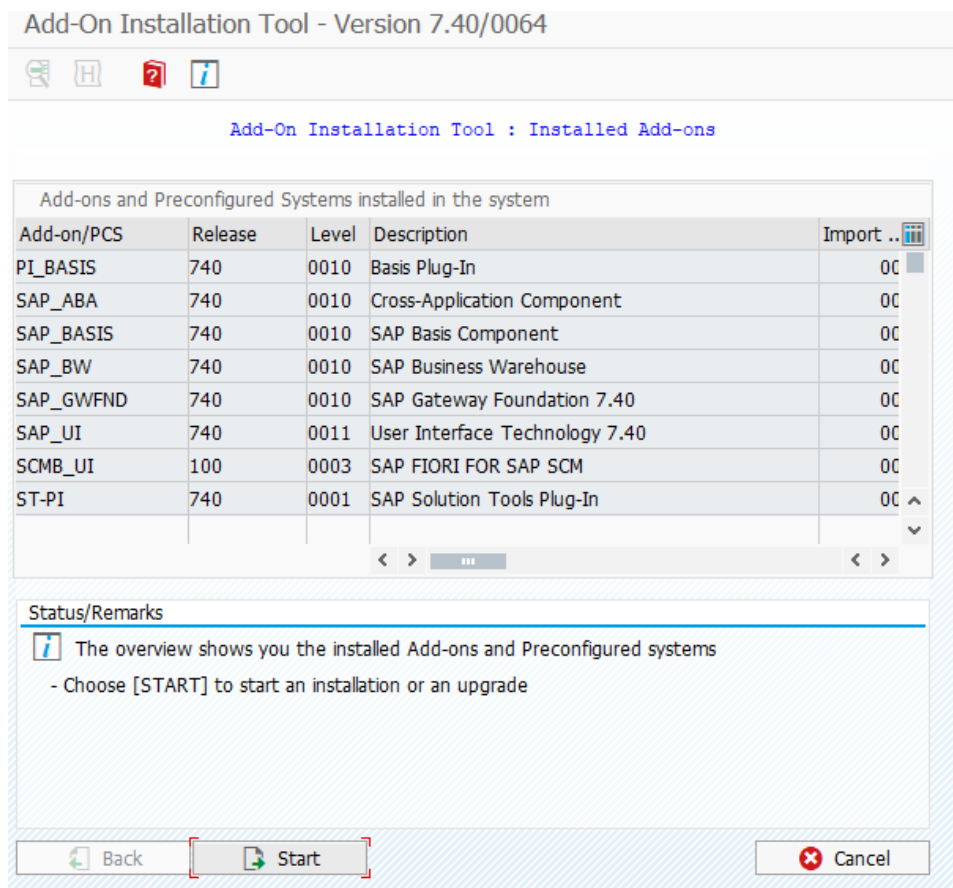


Рисунок 4 – Запуск инсталляции ABAP-агента

- 6) В появившемся окне выбрать компонент GAZIS (SafeERP ABAP Agent), после чего нажать кнопку «Continue» (рис. 5).

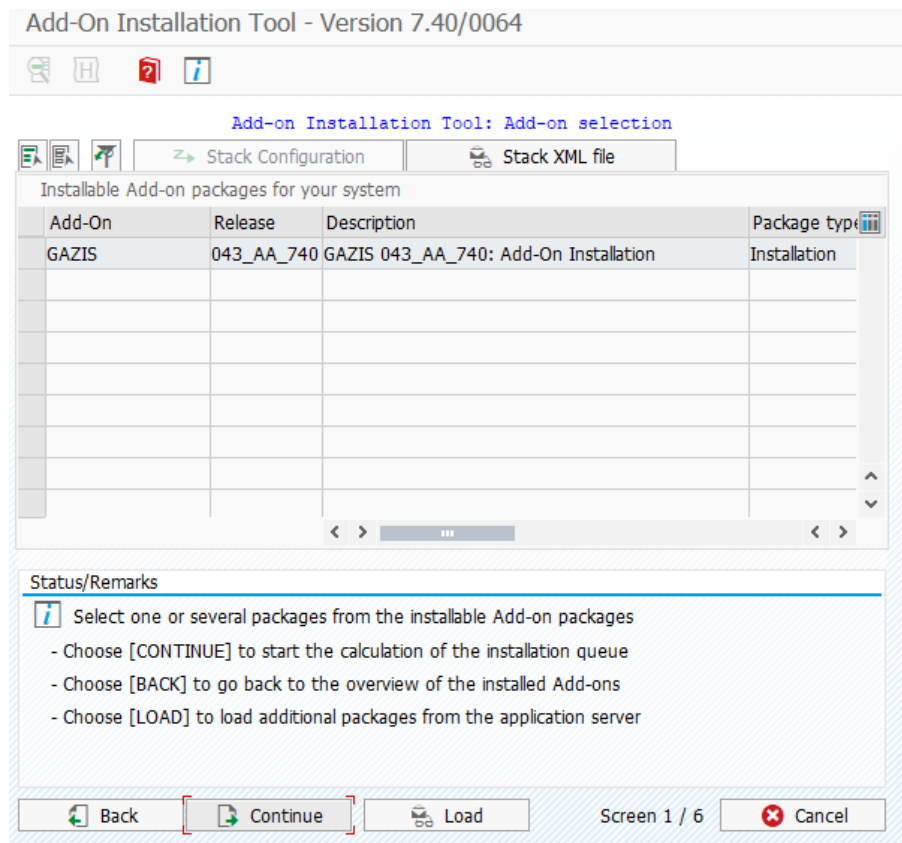


Рисунок 5 – Выбор компонента для инсталляции АВАР-агента

7) В открывшемся окне нажать кнопку «Continue» (рис. 6).

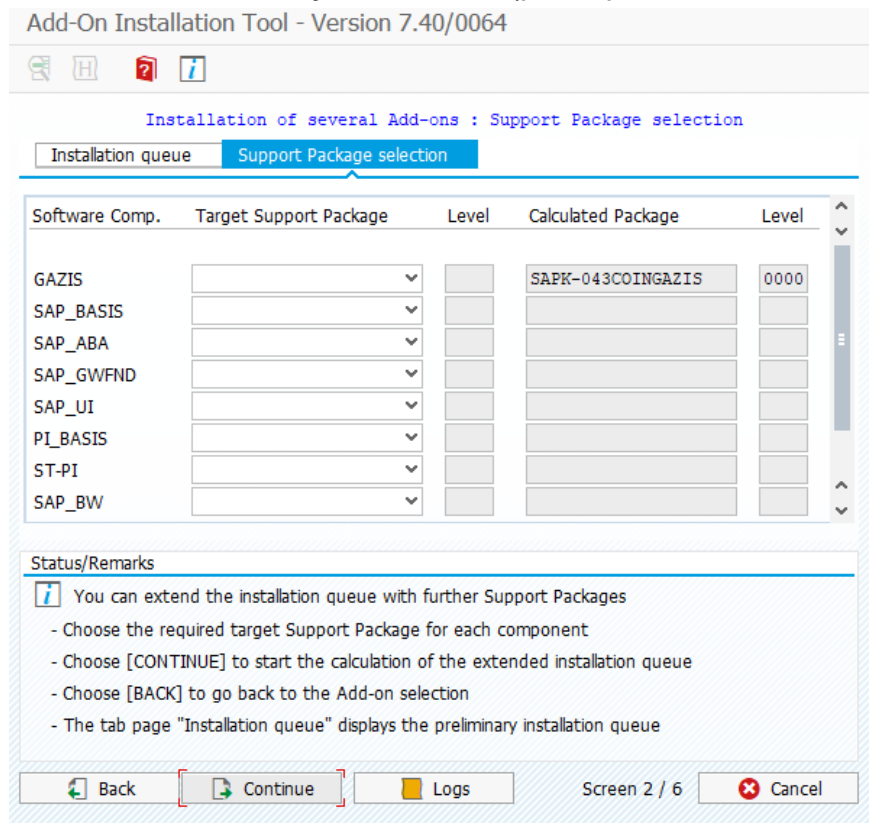


Рисунок 6 – Активация пакета для инсталляции АВАР-агента

8) В следующем окне нажать кнопку «Continue» (рис. 7).

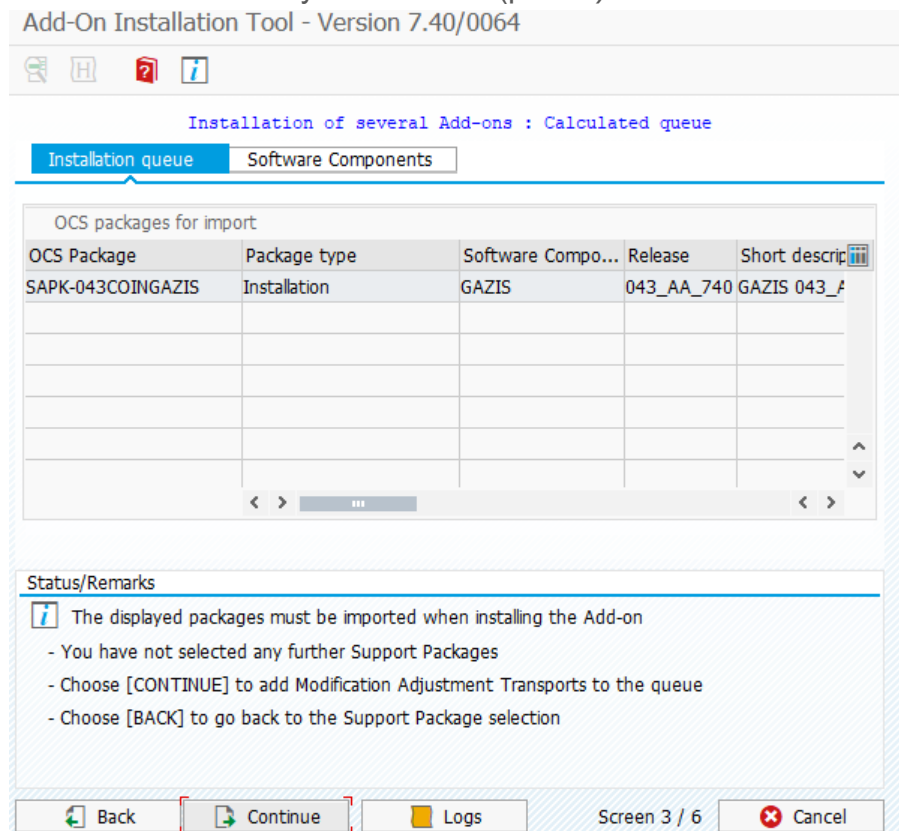


Рисунок 7 – Инсталляция АВАР-агента

9) При получении сообщения «Следует ли добавить переносы сравнений модификаций в очередь инсталляции?» необходимо нажать кнопку «No» (рис. 8).

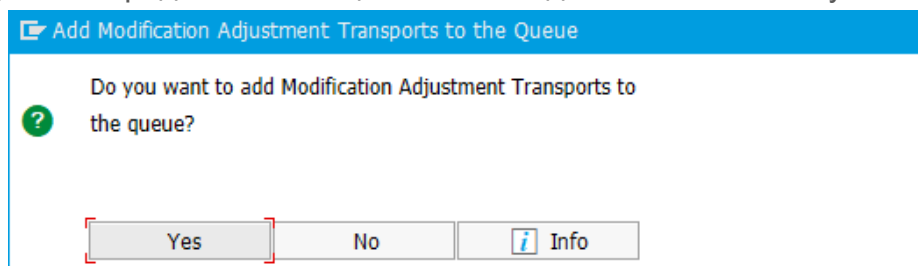


Рисунок 8 – Добавление переносов сравнения

10) В появившемся окне нажать кнопку  и ждать окончания установки агента (рис. 9).

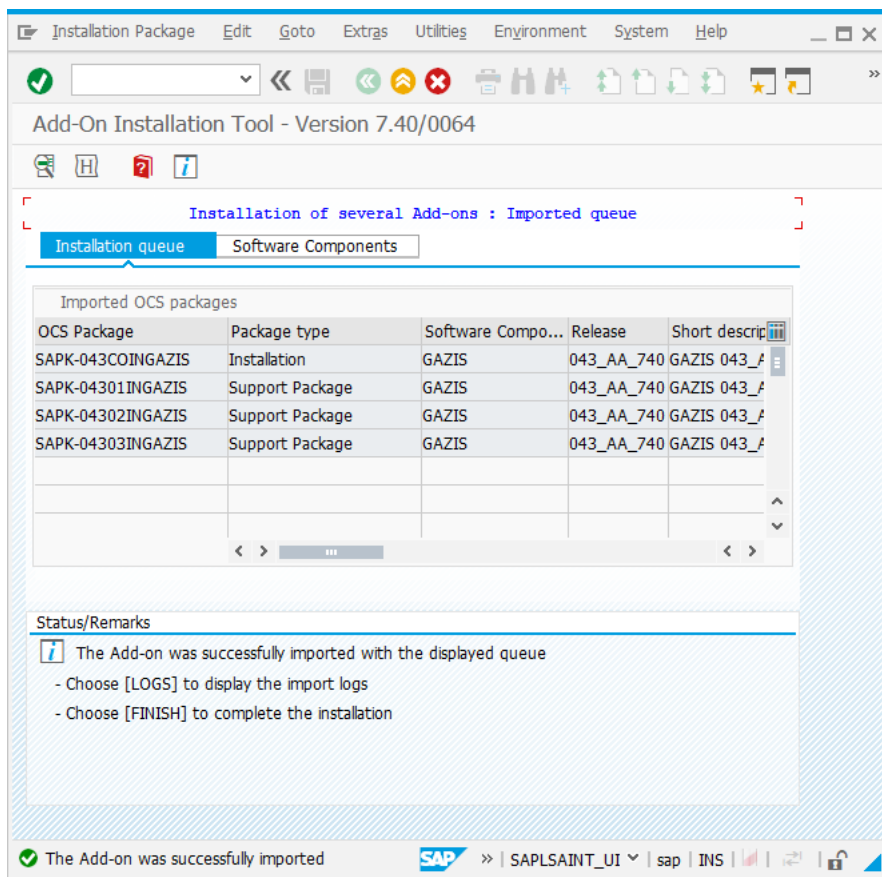


Рисунок 9 – Установка ABAP-агента

11) После успешной установки нажать кнопку «Finish» (рис. 10).

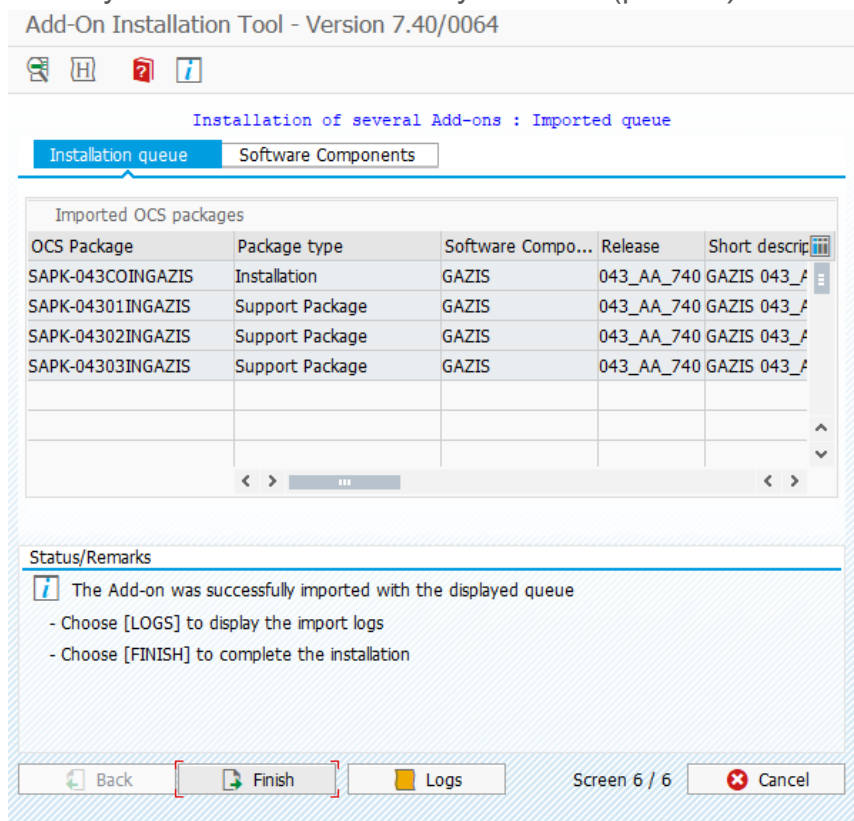


Рисунок 10 – Сообщение о завершении инсталляции

3.1.2. Установка Java-агента

Для установки Java-агента ПК «SafeERP Security Suite» необходимо выполнить следующие действия:

- 1) На сервере управления отредактировать файл «RegInfo». Подключиться к серверу управления и в файл «Reginfo» добавить следующую строку: «P TP=SAFEERP_JAVA_AGENT HOST=<Server> ACCESS=* CANCEL=*». Вместо <Server> указать имя или IP-адрес хоста, на котором будет установлен Java-агент.
- 2) Создать пользователя на сервере управления, как указано в пункте 3.1.2
- 3) Создать RFC-соединение от агента к серверу управления.
- 4) Подключиться к SAP NetWeaver AS Java и зайти в NWA, создать RFC-соединение с сервером управления («Configuration» -> «Infrastructure» -> «Destinations») (рис. 11). В открывшемся окне нажать кнопку «Create», в открывшемся диалоге задать имя сервера управления, номер системы, имя «Gateway service» и данные аутентификации (пользователь, созданный согласно перечислению 2).

Destination List

Create... Remove Remove All Refresh

Destination	Destination Type
DASdefault	HTTP Destination
QAS	RFC Destination

Destination Detail

Edit Ping Destination

RFC Destination QAS

Connection and Transport Logon Data Specific Data

Connection

Load Balancing: ☐ Yes ☒ No

Local System Connection: ☐

Target Host: 10.10.58.36

System Number: 00

System ID: QAS

Message Server:

Message Server Service:

Logon Group:

Gateway Host: 10.10.58.36

Gateway Service: sapgw00

SNC

SNC: ☐ Active ☒ Inactive

QoP: 3: Privacy Protection

SNC Partner Name:

Рисунок 11 – Созданное соединение на агенте SafeERP

- 5) Создать адаптер ресурсов.
Для создания адаптера ресурсов необходимо в меню «Configuration» -> «Infrastructure» -> «Application Resources: Overview» (рис. 12) выбрать пункт «Create New Resource» -> «New Resource Adapter» (рис. 13). В строке «Template» выбрать «SAPJRATemplate», в строке «Application» указать любое имя.

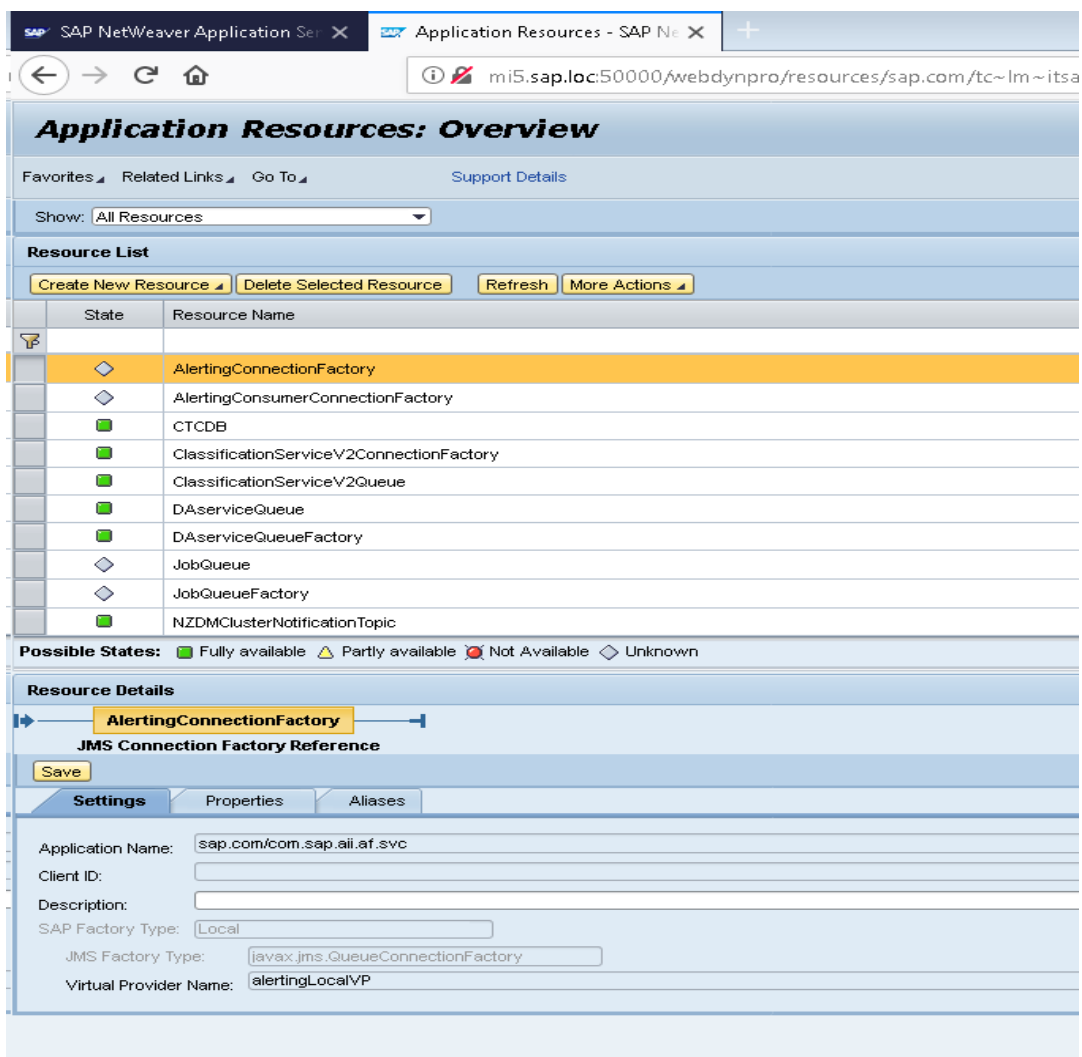


Рисунок 12 – Интерфейс «Application Resources: Overview»

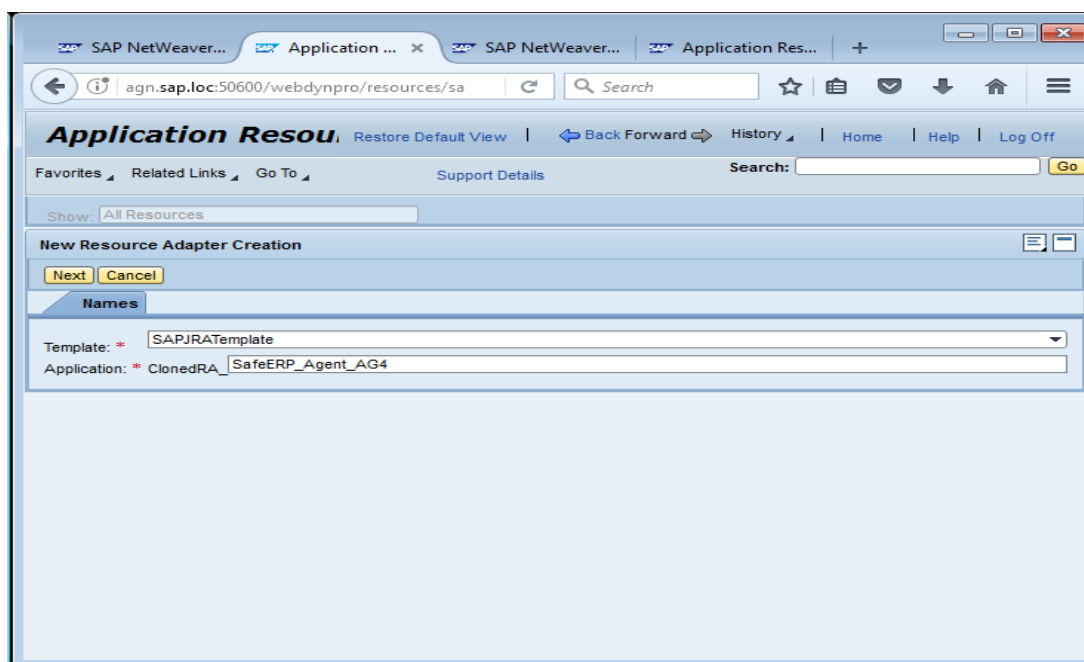


Рисунок 13 – Создание нового адаптера ресурсов

- 6) Далее нажать кнопку «Next». Во вкладке «Settings» указать имя в строке «JNDI name» (рис. 14).

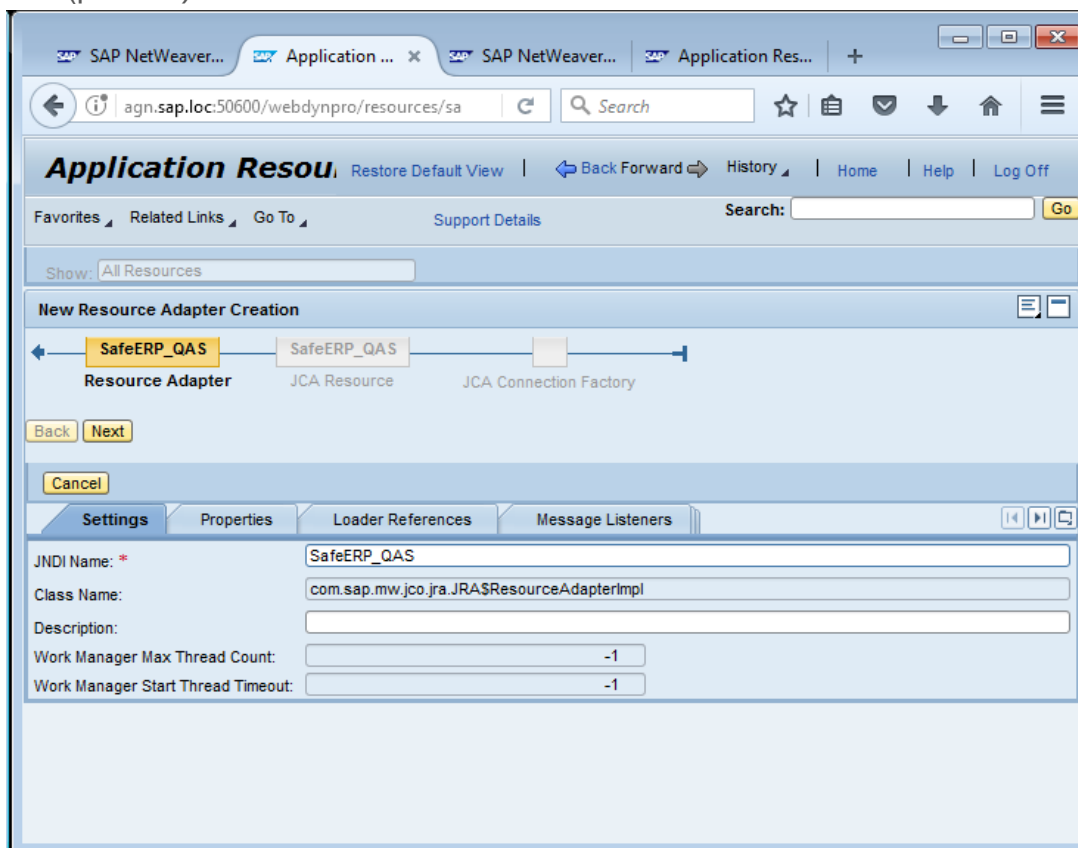


Рисунок 14 – Вкладка «Settings»

- 7) Во вкладке «Properties» указать значения из таблицы Таблица 1 (рис. 15).

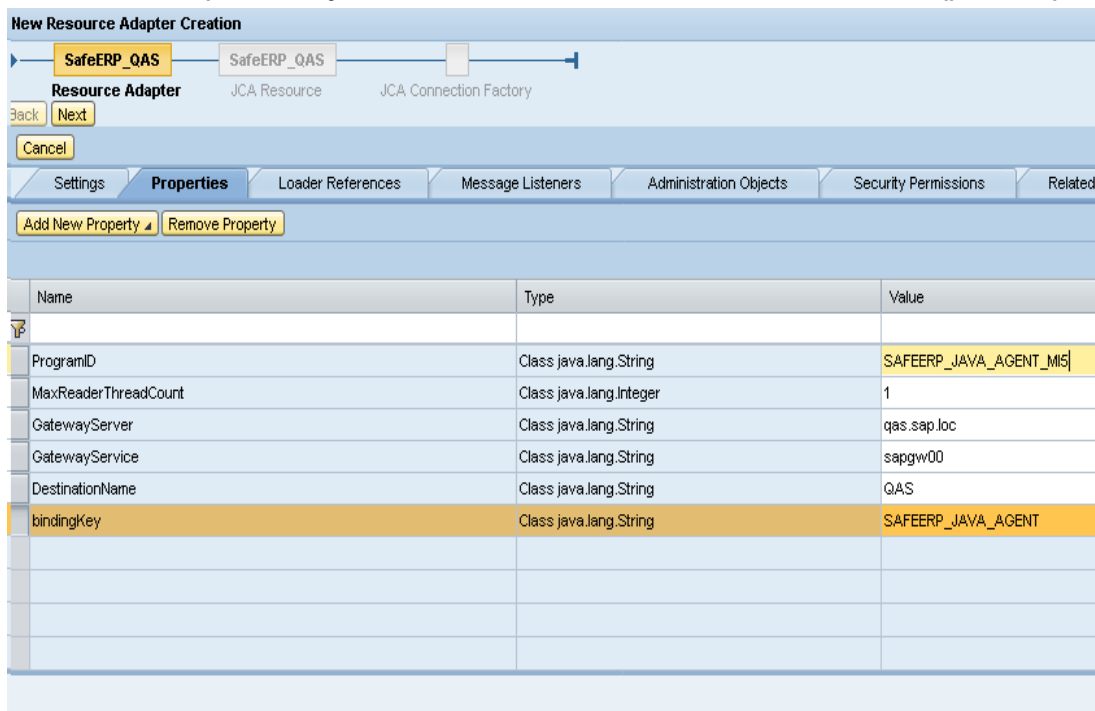


Рисунок 15 – Вкладка «Properties»

Таблица 1 – Значения для параметров вкладки «Properties»

Имя параметра	Значение	Краткое описание
Programm_id	SAFEERP_JAVA_AGENT_<SID>	Имя программы, которую вызывают на шлюзе
MaxReader ThreadCount	1	
GatewayServer	<Имя сервера>	Имя сервера, на котором установлен сервер управления
GatewayService	<Имя сервиса>	Имя сервиса для сервера управления
DestinationName	<Имя RFC>	Имя RFC, созданного согласно перечислению 3
bindingKey	SAFEERP_JAVA_AGENT	Внутренняя программа-агент SafeERP

- 8) Перейти на вкладку «Message Listeners», два раза нажать левой клавишей мыши на строку «com.sap.mw.jco.jra.SynchronousMessageListener», в столбце «Name» указать «SafeERPJavaAgentMB», заменить в разделе «Element Name» параметр «Function name» на «BindingKey» со значением SAFEERP_JAVA_AGENT (рис. 16).

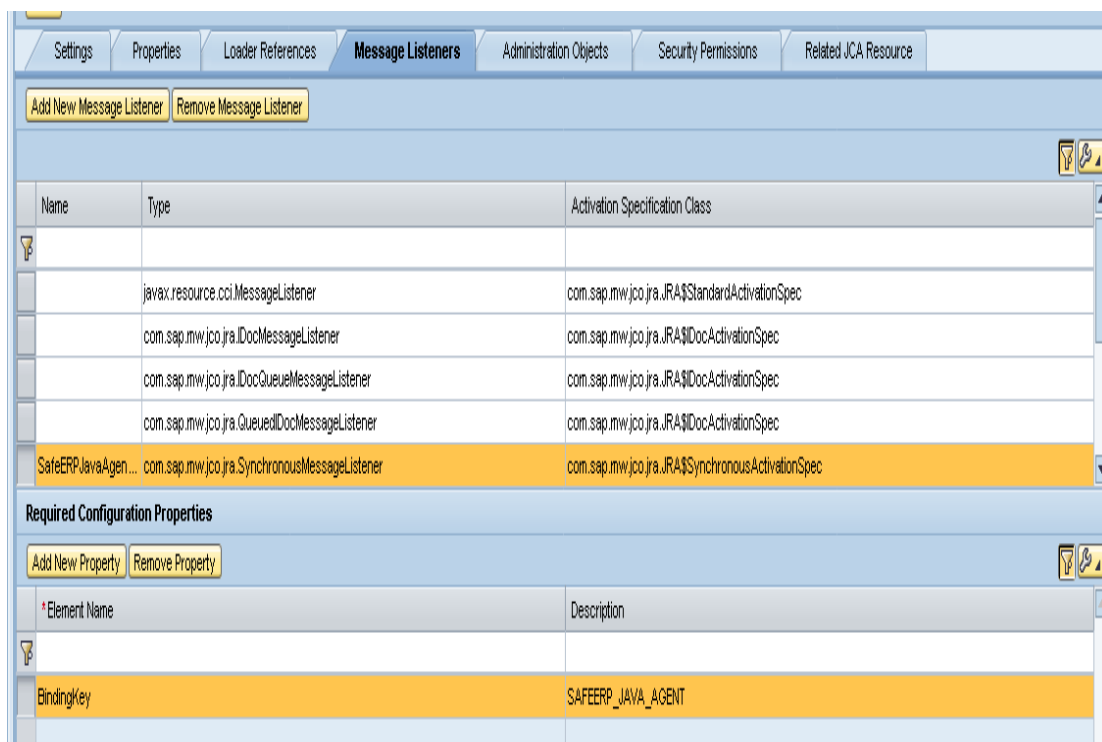


Рисунок 16 – Вкладка «Message Listeners»

- 9) Нажать кнопку «Next» (аналогично в появившемся окне «Related JCA Connection Factories» (рис. 17)).

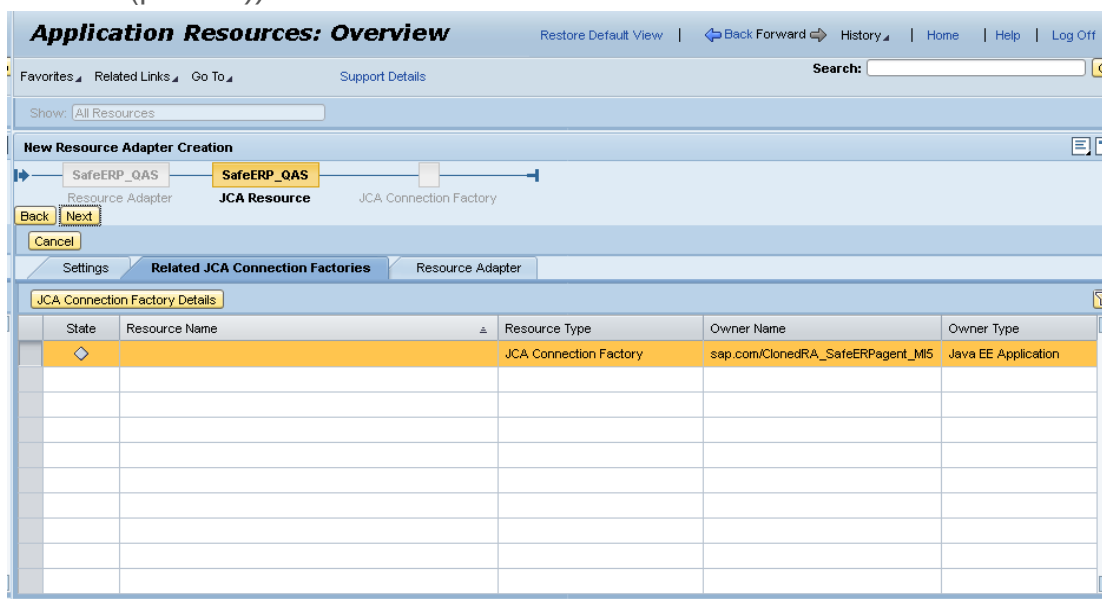


Рисунок 17 – Окно «Related JCA Connection Factories»

- 10) Во вкладке «Namespace» задать имя для «JCA Connection Factory» (рис. 18).

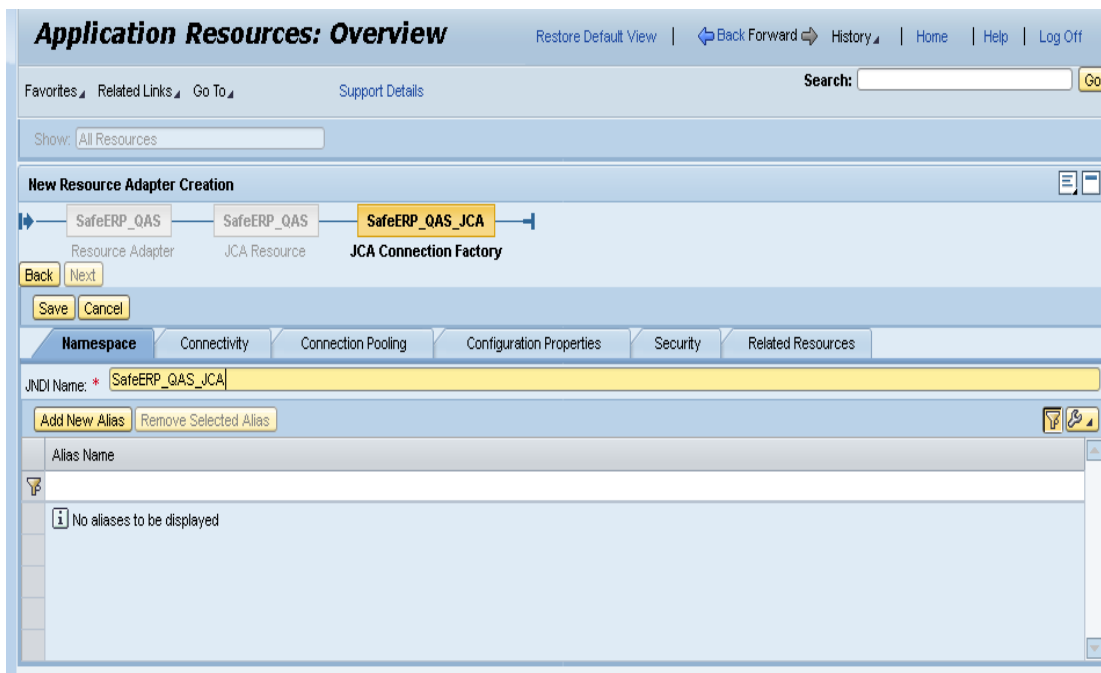


Рисунок 18 – Создание «JCA Connection Factory»

11) Перейти на вкладку «Connection Pooling» (рис. 19) и указать параметры согласно данным из таблицы 2.

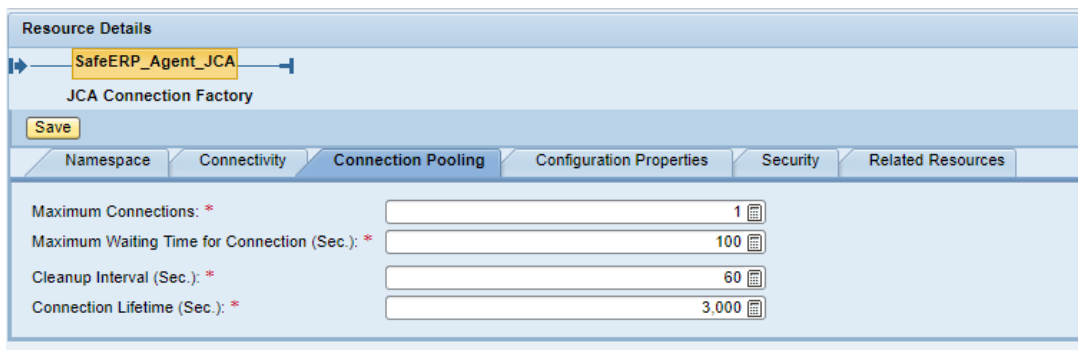


Рисунок 19 – Вкладка «Connection Pooling»

Таблица 2 – Значения для параметров вкладки «Connection Pooling»

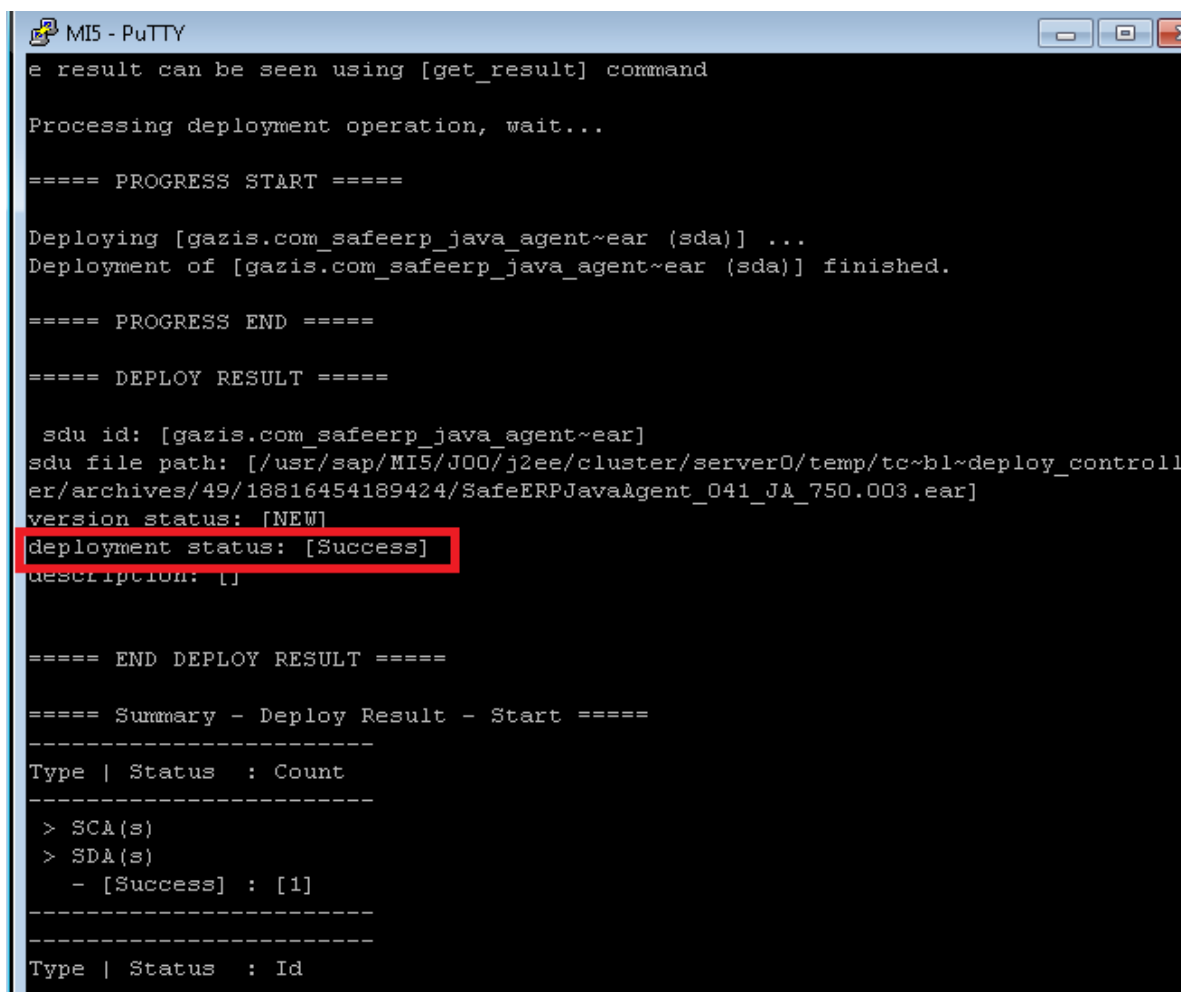
Параметр	Значение
Maximum Connections	1
Maximum Waiting Time for Connection (Sec)	100
Cleanup interval (Sec)	60
Connection Lifetime (Sec)	3000

12) Перейти на вкладку «Configuration Properties» и добавить параметры «gatewayServer», «gatewayService» со значениями из таблицы 1 (рис. 20).



- ```
MIS - PuTTY
```
- ```
*****  
*****  
*****  
#####  
#####  
#####  
#####  
#####  
#####  
#####  
#####  
#####  
#####  
#####  
#####  
#####  
#####  
  
Telnet Administration  
SAP Java EE Application Server v7.40  
  
User name: Administrator  
Password:  
  
Welcome to server node 2556050.  
  
>deploy /usr/sap/SafeERPJavaAgent_041_JA_750.003.ear
```

Результат успешной установки показан на рис. 22.



```
MI5 - PuTTY
e result can be seen using [get_result] command

Processing deployment operation, wait...

===== PROGRESS START =====

Deploying [gazis.com_safeerp_java_agent~ear (sda)] ...
Deployment of [gazis.com_safeerp_java_agent~ear (sda)] finished.

===== PROGRESS END =====

===== DEPLOY RESULT =====

sdu id: [gazis.com_safeerp_java_agent~ear]
sdu file path: [/usr/sap/MI5/J00/j2ee/cluster/server0/temp/tc~bl~deploy_controll
er/archives/49/18816454189424/SafeERPJavaAgent_041_JA_750.003.ear]
version status: [NEW]
deployment status: [Success]
description: []

===== END DEPLOY RESULT =====

===== Summary - Deploy Result - Start =====
-----
Type | Status : Count
-----
> SCA(s)
> SDA(s)
- [Success] : [1]
-----
Type | Status : Id
-----
```

Рисунок 22 – Успешная установка Java-агента

Далее следует отредактировать роль Java-агента. Для этого необходимо войти в интерфейс редактирования роли на сервере агента и добавить в роль «SafeERPAgentRole» полномочия на разрешенные действия, указанные в таблице 3.

Таблица 3 – Полномочия на разрешенные действия для роли SafeERPAgentRole

Тип	Сервис/Приложение	Имя
J2EE	safeerp_java_agent~ear	SafeERPJavaAgentAccess
UME	configuration	ACCESS_CFGMANAGER_ACTION
UME	safeerp_java_agent~action s	ReadMIITablesAction
UME	safeerp_java_agent~action s	ReadEPTablesAction
UME	safeerp_java_agent~action s	ReadUMETablesAction
UME	safeerp_java_agent~action s	ReadBCTablesAction

Далее следует активировать кнопку «Save» (рис. 23).

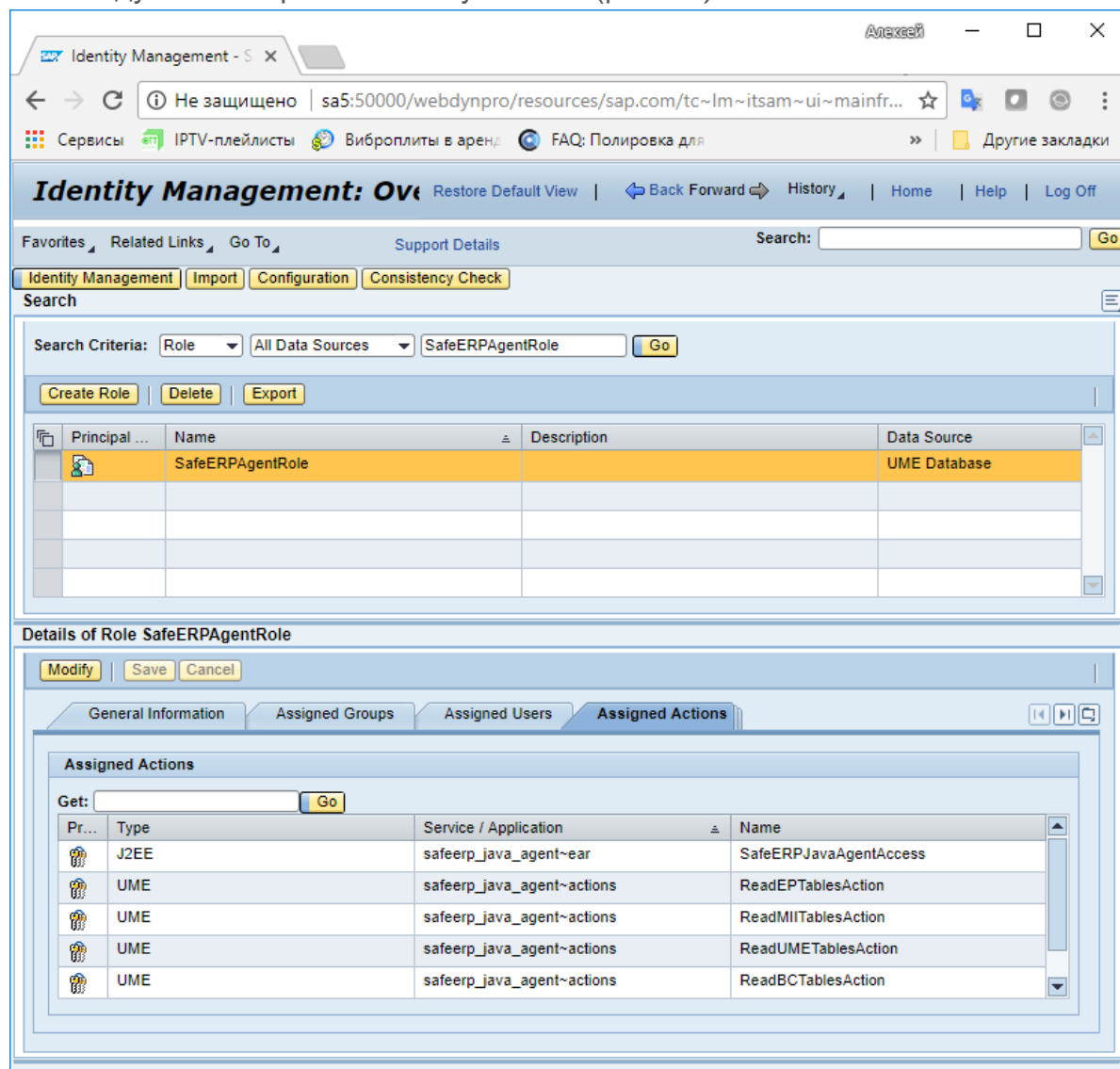


Рисунок 23 – Добавление действий в роль SafeERPAgentRole

3.1.3. Установка ВО-агента

Для установки SAP ВО-агента ПК «SafeERP Security Suite» необходимо выполнить следующие действия:

- 1) Создать пользователя на веб-сервере Tomcat.

Для создания пользователя на веб-сервере Tomcat необходимо отредактировать конфигурационный файл «tomcat-users.xml», добавив в него следующие строки: «<role rolename="manager-gui"/> <user username="tomcat" password="tomcat" roles="managergui"/>». Файл находится по следующему пути: <директория, в которую установлен Tomcat> /conf.

- 2) Перезапустить настройки на веб-сервере Tomcat.

Для активации выполненных настроек согласно предыдущему перечислению необходимо выполнить перезапуск веб-сервера Tomcat. Для этого необходимо перейти в директорию, в которой установлен пользователь, и выполнить следующие команды:

- ./bin /shutdown.sh;
- ./bin /startup.sh.

3) Загрузить агент на сервер SAP BO.

Для загрузки файла на сервер необходимо скопировать файл из дистрибутива (SafeERP_BOAgent.war) на сервер приложения, например, в директорию, в которую установлен пользователь «Tomcat». В браузере выполнить вход в приложение «Manager App» на сервере Tomcat, для этого в адресной строке указать <имя сервера SAPBO>: <портTomcat>//manager/html, например: http://agn.sap.loc:8080/ manager/html.

- 4) Ввести логин и пароль пользователя, созданного согласно перечислению 1, в нижней части открывшегося окна в разделе «Deploy» нажать кнопку «Выберите файл» (рис. 24). Выбрать ранее сохранённый файл SafeERP_BOAgent.war (рис. 25). Нажать кнопку «Deploy».

Deploy

Deploy directory or WAR file located on server

Context Path (required):

XML Configuration file URL:

WAR or Directory URL:

Deploy

WAR file to deploy

Select WAR file to upload Файл не выбран

Deploy

Рисунок 24 – Интерфейс загрузки приложения

WAR file to deploy

Select WAR file to upload SafeERP_...gent.war

Deploy

Рисунок 25 – Интерфейс установки приложения

- 5) После успешной установки в разделе «Applications» проверить наличие приложения «SafeERP_BOAgent» (рис. 26).

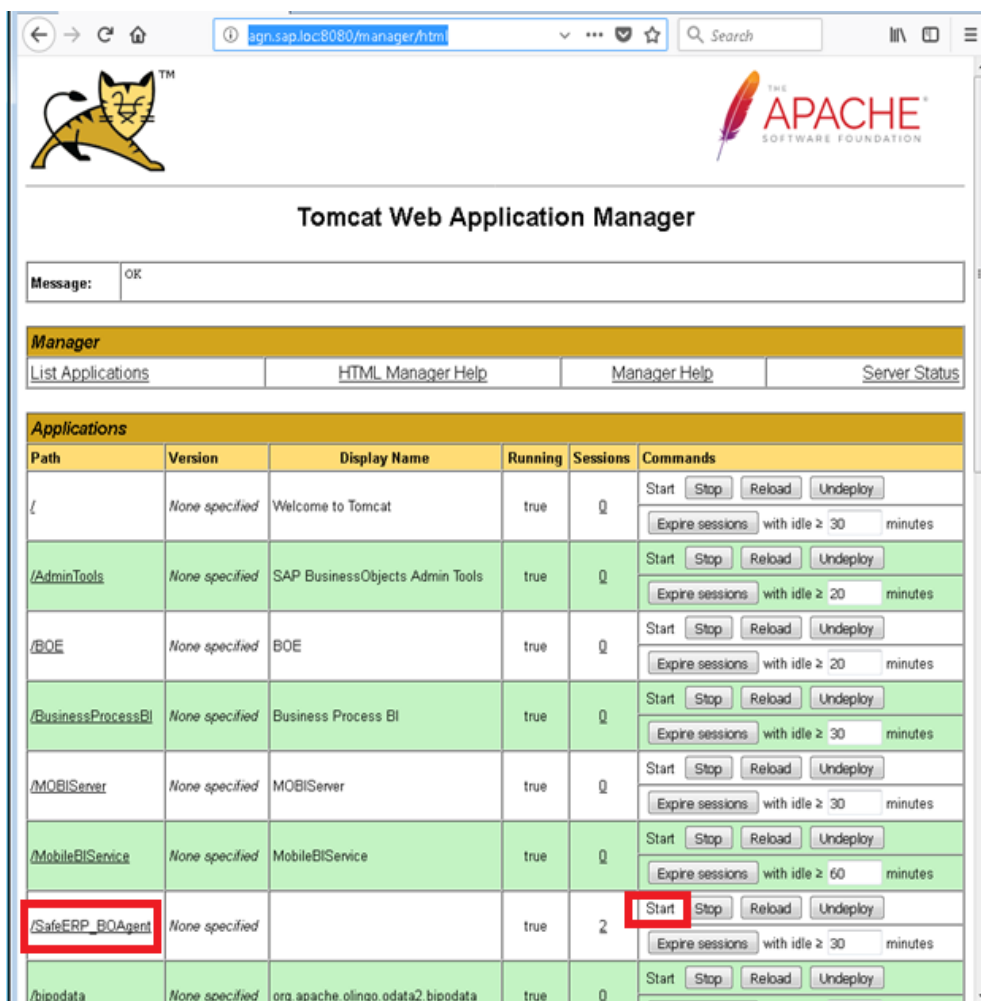


Рисунок 26 – Проверка установленного приложения

3.1.4. Установка HANA-агента

Для установки HANA-агента ПК «SafeERP Security Suite» необходимо выполнить следующие действия:

- 1) Запустить приложение «SAP HANA Studio», выполнить соединение с системой SAP HANA, в которую предполагается установка HANA-агента. Развернуть меню нажатием правой клавиши мыши на названии системы, выбрать пункты меню «Lifecycle Management» -> «Application Lifecycle Management» -> «Home» (рис. 27), в появившемся окне выбрать учётные данные пользователя с полномочиями sap.hana.xs.lm.roles::Administrator (рис. 28).

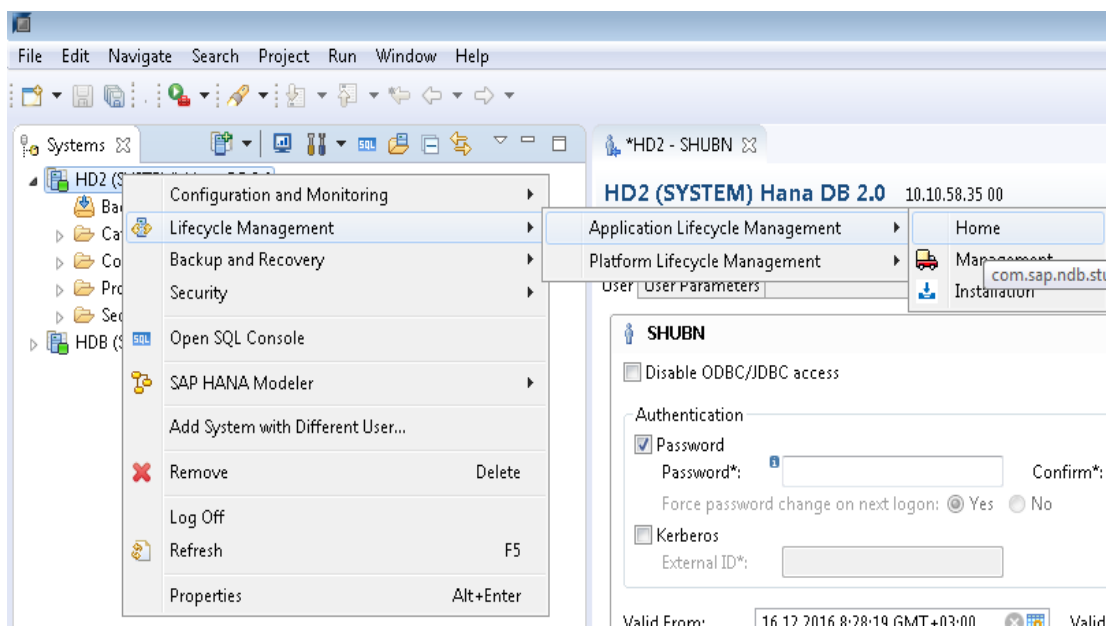


Рисунок 27 – Интерфейс SAP HANA Studio

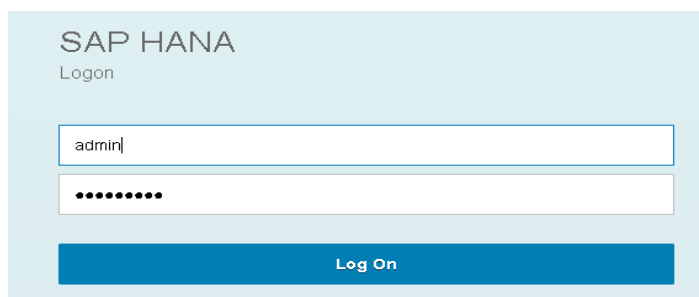


Рисунок 28 – Окно авторизации в «Application Lifecycle Management»

2) В появившемся окне выбрать раздел «Delivery Units» (рис. 29).

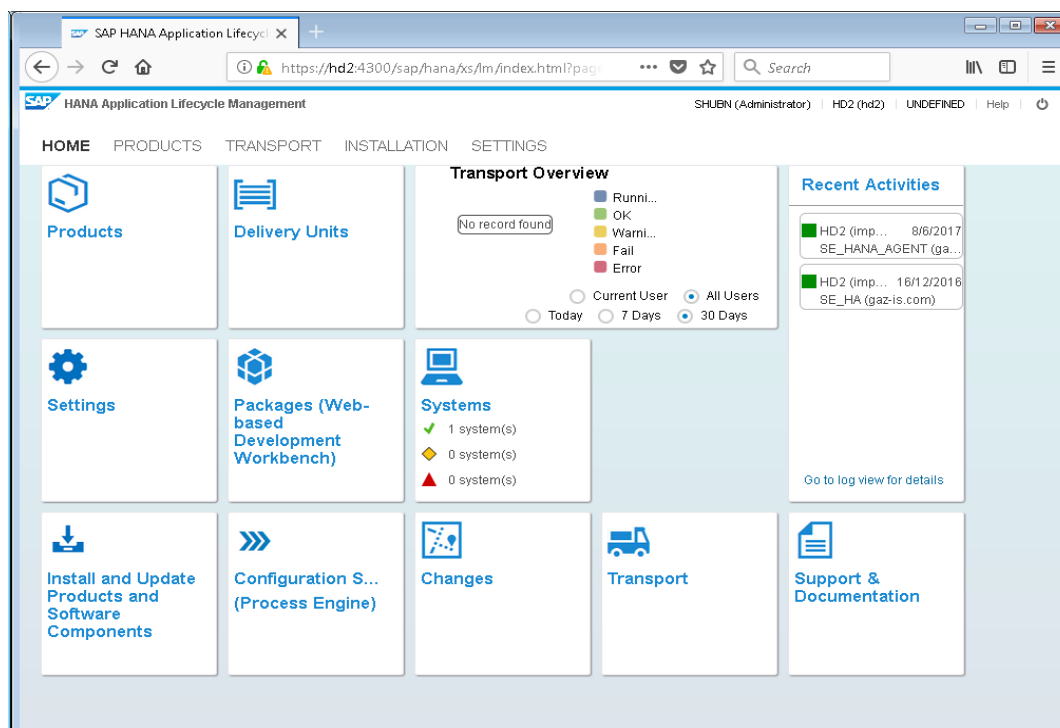


Рисунок 29 – Интерфейс Application Lifecycle Management

- 3) Выполнить импорт продукта ПК «SafeERP Security Suite». Для этого необходимо нажать кнопку «Import», указать путь до файла с агентом (находится на установочном диске), нажав кнопку «Browse», и выполнить загрузку, нажав кнопку «Import» (рис. 30).

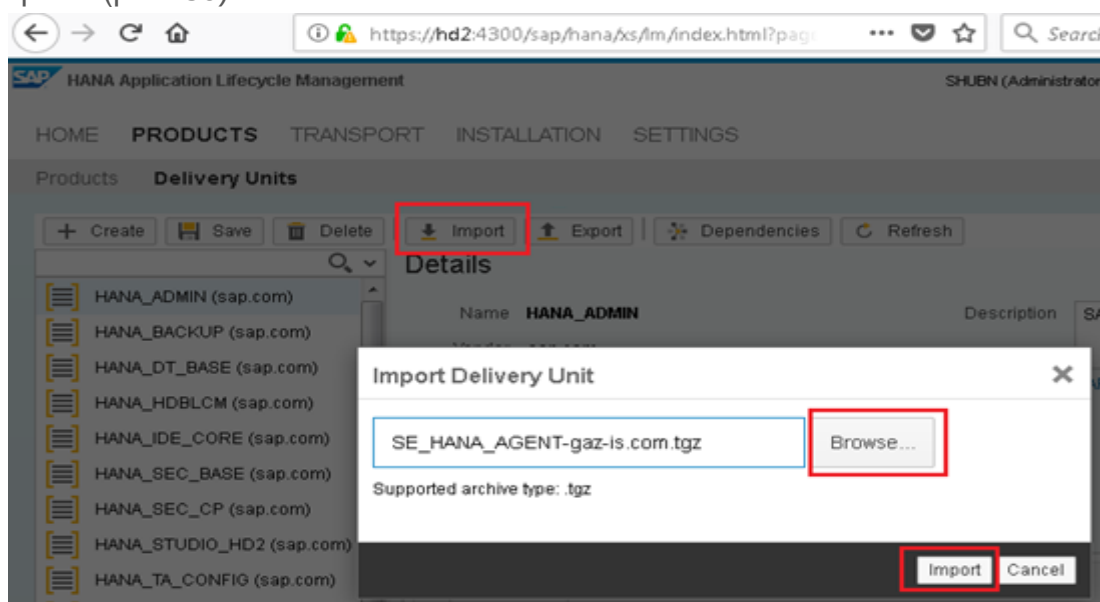


Рисунок 30 – Интерфейс загрузки приложения HANA-агента

- 4) Подтвердить загрузку компонентов, которые появятся в следующем окне, нажав кнопку «Import» (рис. 31).

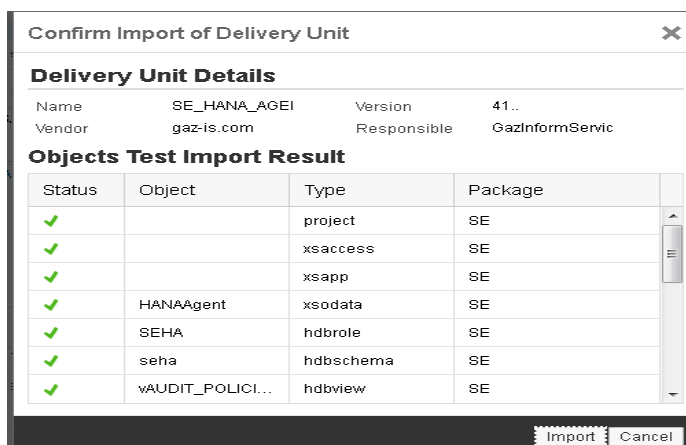


Рисунок 31 – Подтверждение загрузки компонентов

При успешном импорте появится надпись в нижней части окна об успешном завершении задачи (рис. 32).

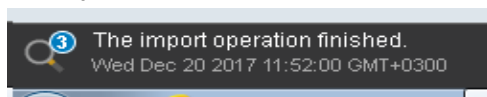


Рисунок 32 – Подтверждение успешного импорта

3.2. Создание системных УЗ агентов ПК «SafeERP Security Suite»

3.2.1. Создание пользователя на ABAP-агенте

Для создания пользователя (для RFC-соединения) в рабочем манданте системы необходимо выполнить следующие действия:

- 1) Запустить транзакцию PFCG, выполнить загрузку роли Z_SAFEERP_AGENT из комплекта поставки. Сгенерировать профиль загруженной роли и выйти из транзакции.
- 2) Запустить транзакцию SU01.
- 3) В поле «User» ввести значение «SAFEERPAGENT».
- 4) Выбрать пункты меню «Users» -> «Create».
- 5) На вкладке «Address» в поле «Last name» ввести значение «Safeerp».
- 6) На вкладке «Address» в поле «First name» ввести значение «Agent».
- 7) На вкладке «Logon data» в поле «User Type» выбрать пункт «Communications Data».
- 8) Ввести пароль «Safeerp» в поля «Initial password» и «Repeat password».
- 9) На вкладке «Roles» добавить роль «Z_SAFEERP_AGENT».
- 10) Выбрать пункты меню «Users» -> «Save».

3.2.2. Создание пользователя на Java-агенте

Для создания пользователя на Java-агенте необходимо выполнить следующие действия:

- 1) Запустить приложение «User Management», во вкладке «General Information» создать новую роль с именем «SafeERPAgentRole» (без авторизаций) (рис. 33).

Identity Management: Overview

Favorites ▾ Related Links ▾ Go To ▾ [Support Details](#)

[Identity Management](#) [Import](#) [Configuration](#) [Consistency Check](#)

Search

Search Criteria: Role ▾ All Data Sources SafeERPAgentRole [Go](#)

[Create Role](#) [Delete](#) [Export](#)

Principal Type	Name
Enter a search parameter and choose Go	

Details

[Modify](#) [Save](#) [Cancel](#)

General Information [Assigned Groups](#) [Assigned Users](#) [Assigned Actions](#) [User Mapping for System Access](#)

Unique Name: * SafeERPAgentRole

Display Name:

Location:

Description: SafeERPAgentRole

Unique ID:

Рисунок 33 – Создание пользователя на системе агента

- 2) Создать пользователя «Safeerpage» и присвоить ему ранее созданную роль «SafeERPAgentRole» (рис. 34).

The screenshot displays the 'Identity Management: Overview' interface. At the top, a status bar indicates 'User created'. Below this, there are navigation tabs: 'Identity Management', 'Import', 'Configuration', and 'Consistency Check'. A search section allows filtering by 'User' and 'All Data Sources', with a search term 'Safeerpagent' entered. Action buttons include 'Create User', 'Copy to New User', 'Delete', 'Unlock', 'Lock', 'Generate New Password', and 'Export'. A table lists user details:

Principal Type	Status	Logon ID	Name	Department
Agent	Active	Safeerpagent	Agent, SafeERP	

Below the table is the 'Details of User Safeerpagent' section. It includes tabs for 'General Information', 'Account Information', 'Contact Information', 'Additional Information', 'Assigned Roles', 'Assigned Groups', 'User Mapping for System Access', and 'E-mail Signature'. The 'Assigned Roles' tab is active, showing a search for 'SafeERP AgentRole' with the following results:

Principal Type	Name	Description	Data Source
Role	SafeERP AgentRole	SafeERP AgentRole	UME Database

Рисунок 34 – Создание пользователя «Safeerpagent»

3.2.3. Создание пользователя на ВО-агенте

Для создания пользователя на ВО-агенте необходимо зайти в консоль управления системы SAP BO Central Management Console (CMC) и выполнить следующие действия:

- 1) Выполнить вход в консоль SAP BO, набрав в адресной строке браузера следующий адрес: «http://<Имя сервера SAP BO>:<порт SAP BO>/BOE/CMC». В окне входа ввести имя пользователя с правами администратора, выполнить вход (рис. 35).

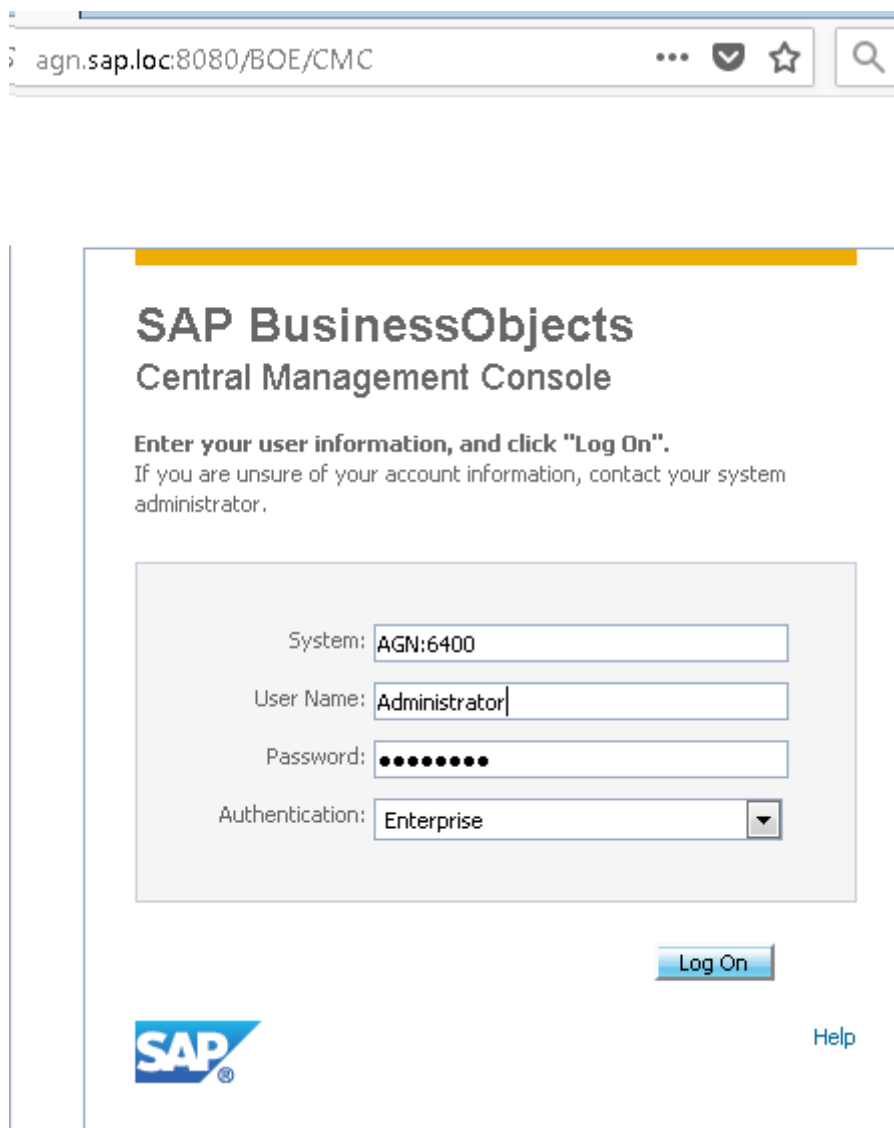


Рисунок 35 – Интерфейс входа в CMC SAP BO

- 2) Открыть раздел «Users and Groups», выбрать группу «Administrators» (рис. 36).
Выбрать на панели инструментов пункт «Create a user».

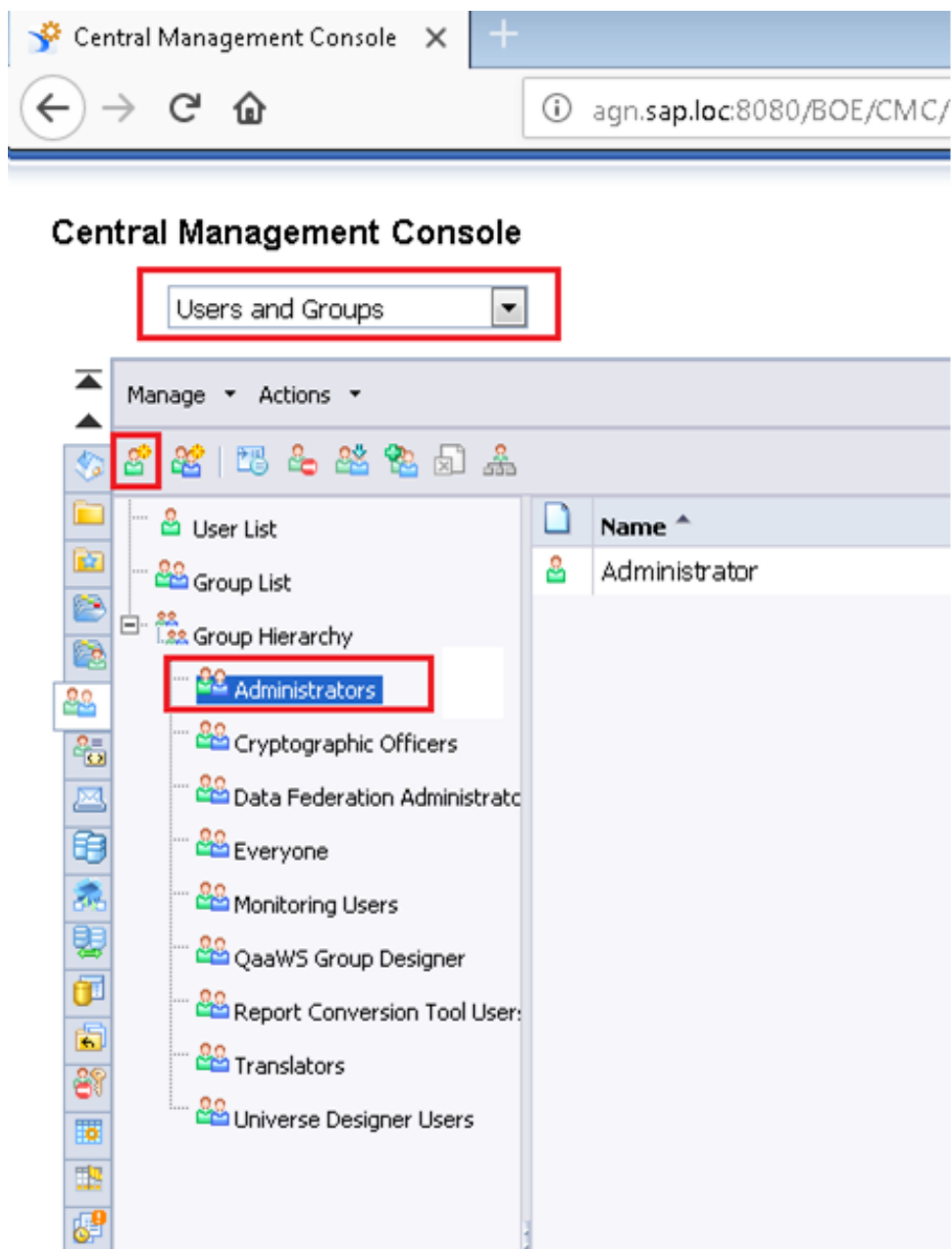


Рисунок 36 – Окно управления пользователями

Поставить флаг в поле «Password never expires», в поле «Account name» ввести значение «SAFEERPAGENT», в поле «Full name» ввести значение «УЗ агента SAFEERP», в поле «Description» ввести «системный пользователь для агента SafeERP» (рис. 37). Нажать кнопку «Create & Close».

New User

Authentication Type: Enterprise

Account Name: SAFEERPAGENT

Full Name: УЗ агента SAFEERP

Email:

Description: СИСТЕМНЫЙ пользователь для агента SafeERP

Enterprise Password Settings

Password: [masked] ☒ Password never expires

Confirm: [masked] ☐ User must change password at next logon

☐ User cannot change password

Access Type

☐ Limited by concurrent session pool

☒ Guaranteed - named user

Create Create & Close Cancel

Рисунок 37 – Окно создания пользователя

3.2.4. Создание пользователя на HANA-агенте

Для создания пользователя в SAP HANA для ПК «SafeERP Security Suite» необходимо выполнить следующие действия:

- 1) Запустить приложение «SAP HANA Studio» и выполнить соединение с системой, в которой выполняется установка HANA-агента. В разделе «Security» -> «Users» нажать пункт «Create a new user» (рис. 38).

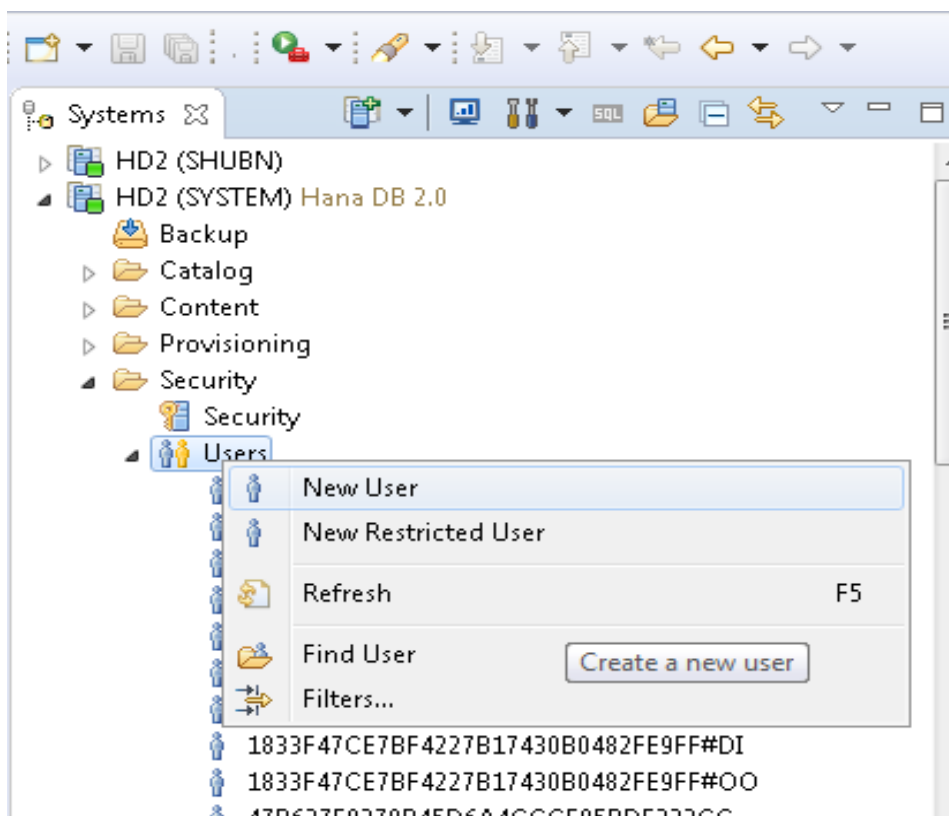


Рисунок 38 – Меню создания пользователя

- 2) В окне справа необходимо записать имя пользователя «SafeERPagent», задать пароль, а также присвоить роль PUBLIC и _gazis_.SEHA::SEHA (рис. 39), после чего нажать кнопку «Применить» .

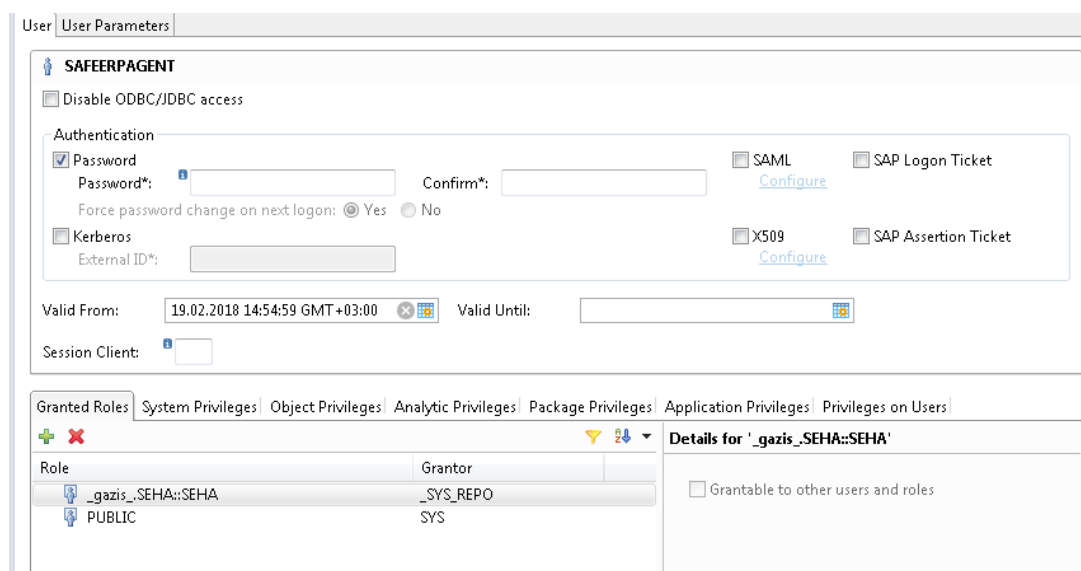


Рисунок 39 – Параметры пользователя

3.3. Установка сервера управления ПК «SafeERP Security Suite»

Для установки сервера управления необходимо выполнить действия, аналогичные приведенным в пункте 3.3.1, вместо файла «SafeERP_nnn_AA_NNN.SAR» следует

использовать файл «SafeERP_nnn_MS_NNN.SAR» (директория на диске \Installation\Server\).

Примечание. При установке сервера управления необходимо установить архиватор для корректного создания отчетов в модуле «Сканер».

3.3.1. Активация BC Set

Для переноса данных в рабочий клиент необходимо выбрать рабочий мандант, в котором будут работать оператор и администратор ПК «SafeERP Security Suite». Действия, описанные в пунктах 3.3.1 – 3.3.7, следует выполнять в том же манданте.

Для активации BC Set необходимо запустить транзакцию scpr20 и выполнить активацию следующих наборов:

- /GAZIS/FIORI;
- /GAZIS/SECS;
- /GAZIS/SEGA;
- /GAZIS/SEPS;
- /GAZIS/SE_COMMON;
- /GAZIS/SREPORT;
- /GAZIS/STGAJAT;
- /GAZIS/APPL_LOG.

Примечание – Во избежание таймаута, активацию набора /GAZIS/SEPS необходимо запускать в фоновом режиме (рис. 40).

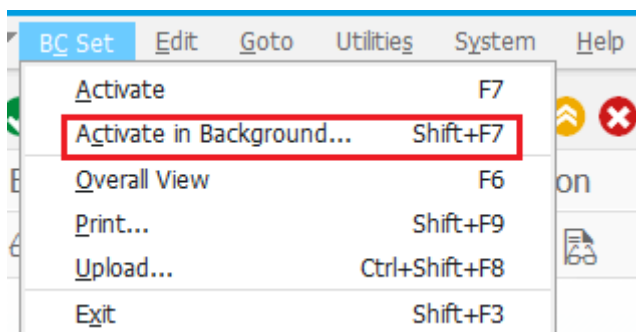


Рисунок 40 – Активация в фоновом режиме BC set

3.3.2. Настройка компонента SAP FIORI

Для настройки интерфейса SAP FIORI необходимо выполнить следующие действия:

- 1) Запустить транзакцию SICF и выполнить активацию ветки сервисов из списка:
 - /sap/bc/ui5_ui5/GAZIS;
 - /sap/opu/odata/gazis;
 - /sap/bc/apc/gazis;
 - /sap/public/opu.
- 2) Запустить транзакцию STC01 и выполнить следующие скрипты:
 - SAP_FIORI_LAUNCHPAD_INIT_SETUP;
 - /UIF/SCHEDULE_LREP_JOB;
 - SAP_FIORI_REFERENCE_APPS_SETUP;

— SAP_GW_FIORI_ERP_ONE_CLNT_SETUP.

- 3) При выполнении скриптов необходимо контролировать описание каждого шага их выполнения и при необходимости корректировать действия «вручную».
- 4) В рабочий мандант импортировать транспортный запрос DMSK904408 (SafeERP Fiori 2020 for SP9).

3.3.3. Активация сервисов

Для активации сервисов необходимо выполнить следующие действия:

- 1) Перейти в транзакцию /N/GAZIS/MAINT_SERVICE.
- 2) Проверить все сервисы, начинающиеся на «/GAZIS/*». Необходимо проверить активность ICF-узлов и системные псевдонимы ICF-узлов.
- 3) Нажать кнопку «Загрузить метаданные».

Примечания:

1. Если сервис не активирован, то необходимо нажать кнопку «ICF-узел», затем нажать кнопку «Активировать».
2. Если не присвоены псевдонимы, то необходимо нажать кнопку «Доб.сист.псевдоним», добавить значение «*имя сервиса*_0001», Alias – LOCAL, установить флаг в столбце «Default system».

3.3.4. Настройка RFC-групп

Для возможности одновременного выполнения процессов сканирования кода необходимо настроить RFC-группы на сервере управления. Для этого следует запустить транзакцию RZ12 и создать новую группу с именем SafeERP, добавив в неё все существующие экземпляры сервера управления. Если экземпляры одна, то необходимо включить только её.

3.3.5. Активация SAP Gateway

Для работы функционала SAP Fiori необходимо активировать технологию подключения устройств SAP Gateway, для этого следует запустить транзакцию SPRO, нажать кнопку «Ссылочное IMG SAP» (рис. 41) и пройти по следующему пути: «SAP NetWeaver» -> «SAP Gateway» -> «OData Channel» -> «Configuration», нажать левой кнопкой мыши на пункт «Activate or Deactivate SAP Gateway» (рис. 42) и выбрать в открывшемся окне нажать кнопку .

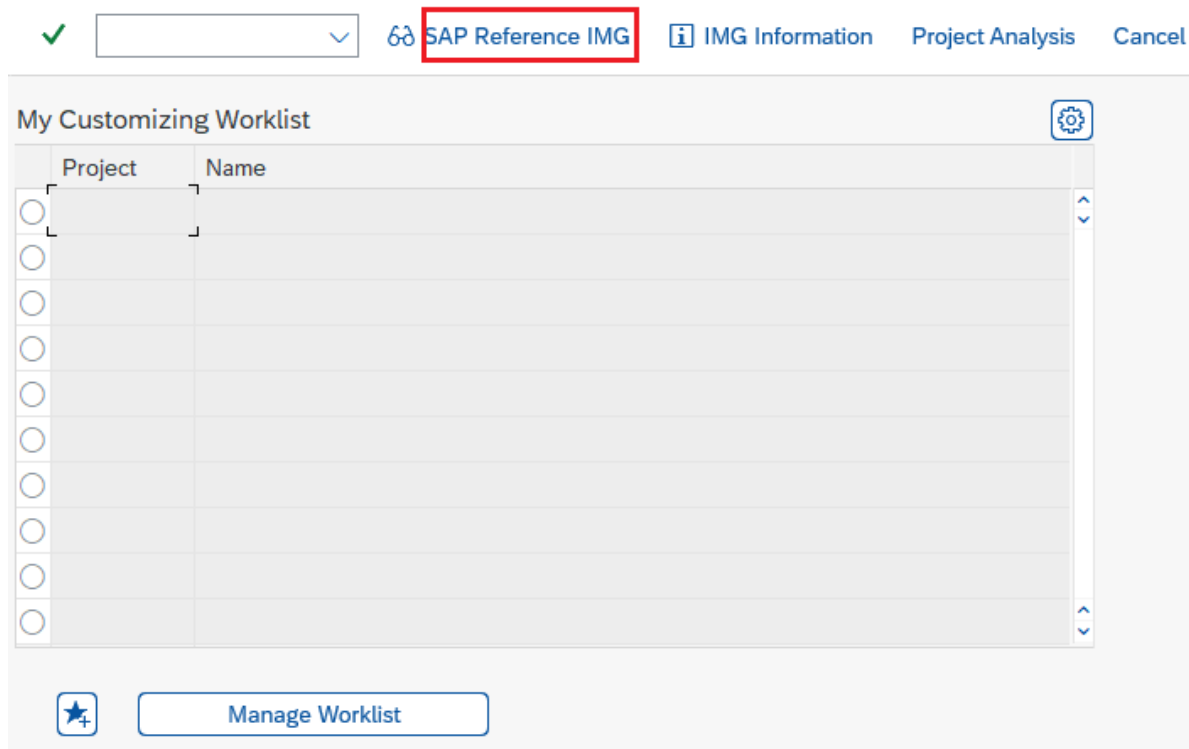


Рисунок 41 – Ссылочное IMG SAP

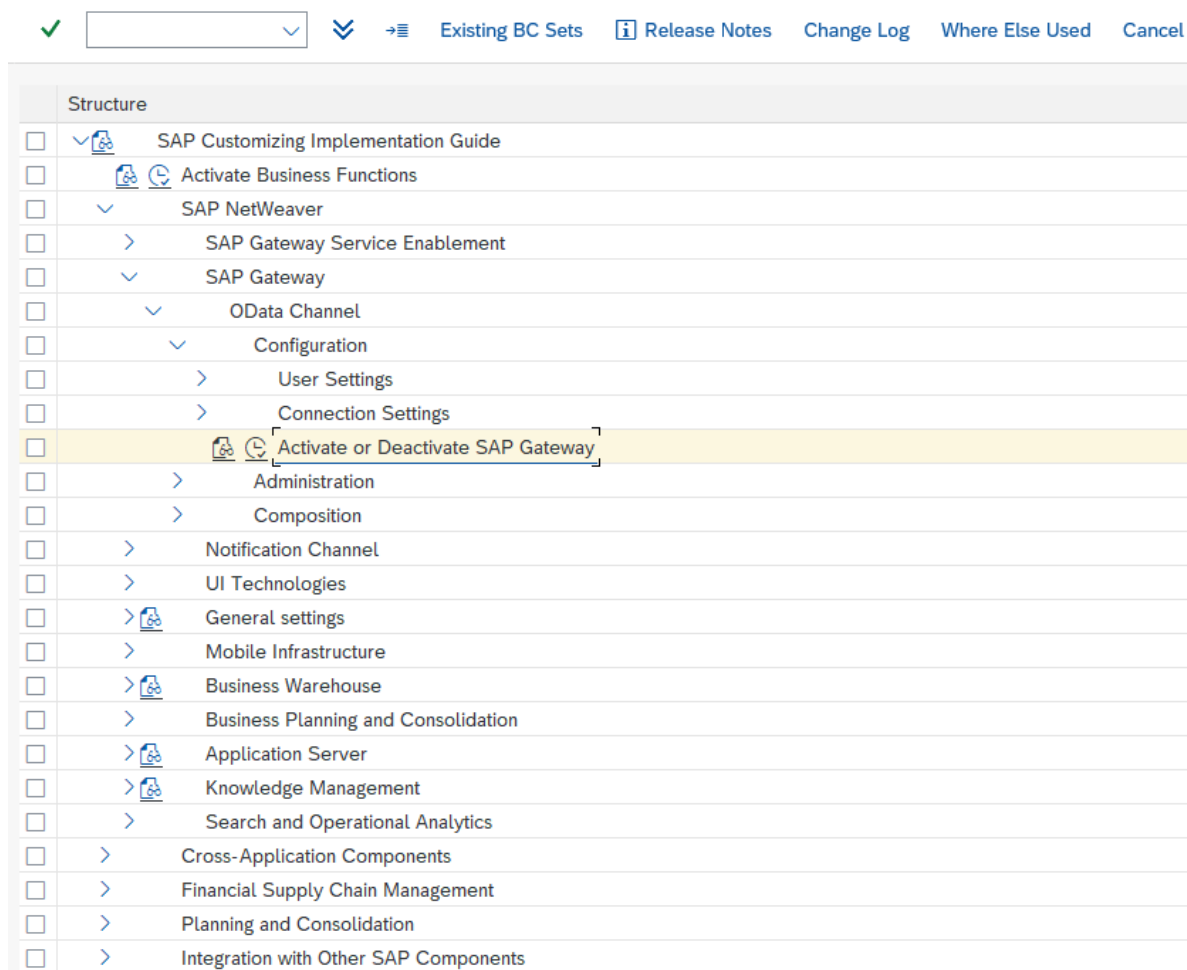


Рисунок 42 – Путь к «Activate or deactivate SAP Gateway»

3.3.6. Создание пользователя с правами оператора ПК «SafeERP Security Suite»

Для создания пользователя с правами оператора ПК «SafeERP Security Suite» необходимо выполнить действия в следующей последовательности:

- 1) Запустить транзакцию SU01.
- 2) В поле «User» ввести идентификатор персонифицированной учетной записи пользователя в соответствии с внутренним регламентом организации.
- 3) Выбрать пункты меню «Users» -> «Create».
- 4) На вкладке «Address» в поле «Last name» и «First name» ввести персональные данные пользователя.
- 5) На вкладке «Logon data» в поле «User Type» выбрать пункт «Dialog».
- 6) Ввести пароль «OPERATOR» в поля «Initial password» и «Repeat password».
- 7) На вкладке «Roles» в поле «Role» ввести название роли: «Z_SAFEERP_OPERATOR».
- 8) Выбрать пункты меню «Users» -> «Save».
- 9) В транзакции PFCG (при необходимости разграничения доступа операторов к системам) создать дополнительную роль, в которой будет указан идентификатор группы, содержащий список систем для определенного оператора/операторов (рис. 43, 44, 45).

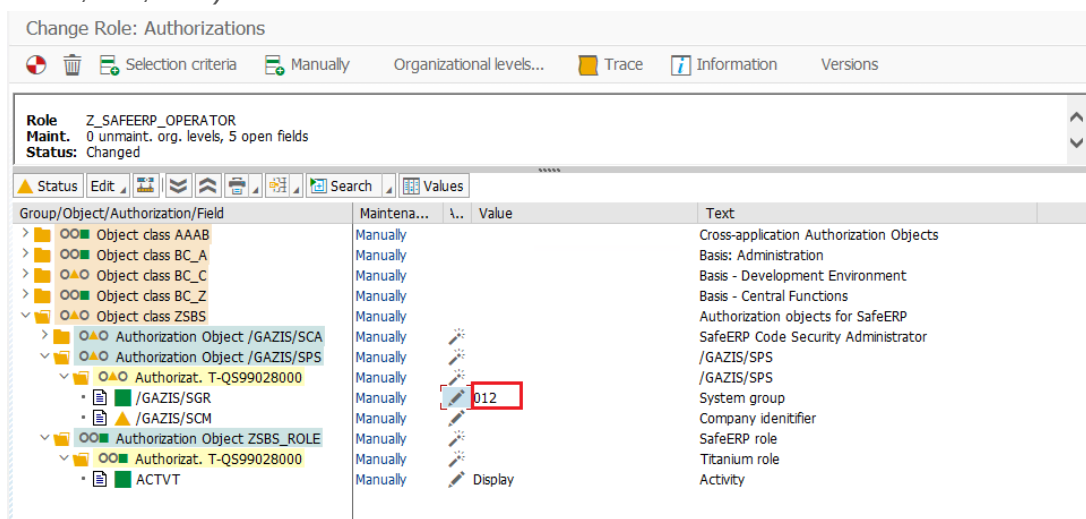


Рисунок 43 – Создание дополнительной роли

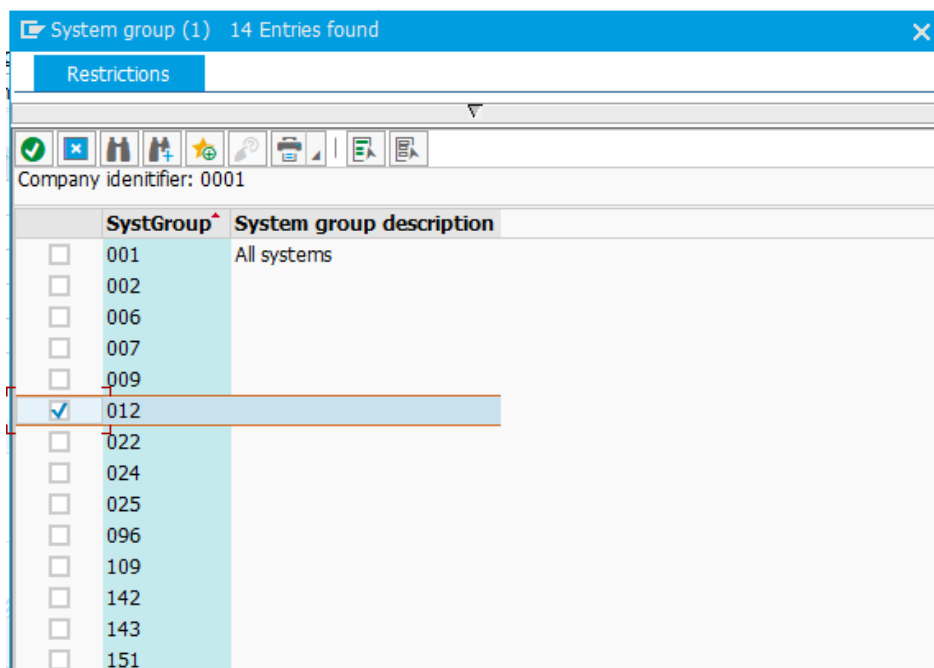


Рисунок 44 – Выбор группы из списка

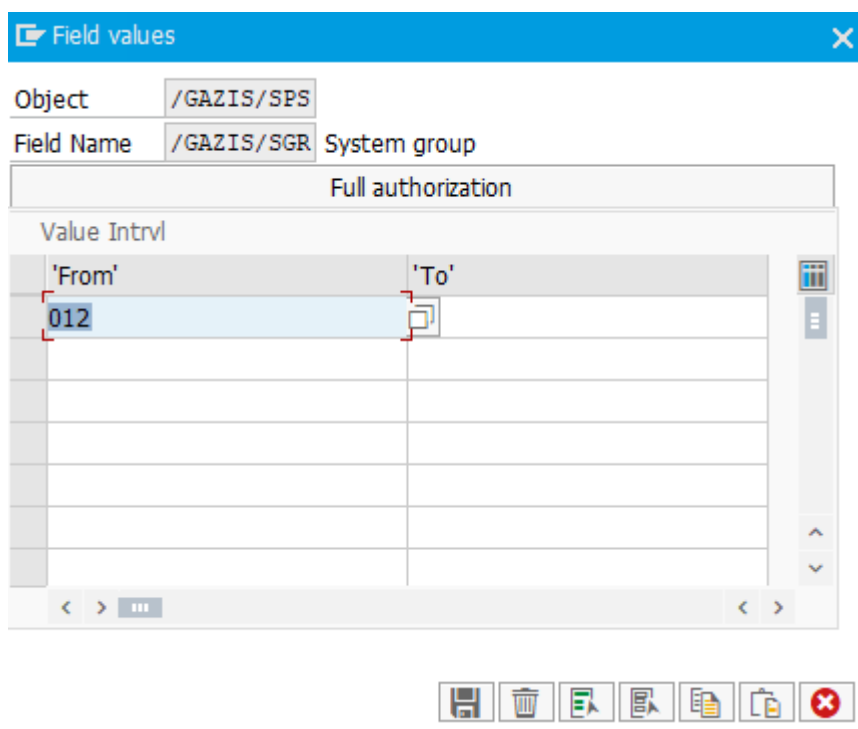


Рисунок 45 – Номер группы из списка

Порядок действий по созданию группы для системы/систем приведен в документе «Руководство администратора».

Присвоить созданную роль оператору, которому должны быть доступны системы из выбранной группы (рис. 46).

User ID	User Name	From	to	In...
OPERATOR-01	Оператор SafeERP	11.05.2021	31.12.9999	
OPERATOR-02	Оператор SafeERP	21.07.2020	31.12.9999	

Рисунок 46 – Итоговый список ролей оператора

3.3.7. Создание пользователя с правами администратора ПК «SafeERP Security Suite»

Для создания пользователя с правами администратора ПК «SafeERP Security Suite» необходимо выполнить действия в следующей последовательности:

- 1) Запустить транзакцию SU01.
- 2) В поле «User» ввести идентификатор персонифицированной учетной записи пользователя в соответствии с внутренним регламентом организации.
- 3) Выбрать пункты меню «Users» -> «Create».
- 4) На вкладке «Address» в поля «Last name» и «First name» ввести персональные данные пользователя.
- 5) На вкладке «Logon data» в поле «User Type» выбрать пункт «Dialog».
- 6) Ввести пароль «ADMIN» в поля «Initial password» и «Repeat password».
- 7) На вкладке «Roles» в поле «Role» ввести название роли: «Z_SAFEERP_ADMINISTRATOR».
- 8) Выбрать пункты меню «Users» -> «Save».

3.3.8. Создание RFC-соединения от сервера управления к ABAP-агенту

Для создания RFC-соединения от сервера управления к ABAP-агенту системы необходимо выполнить действия в следующей последовательности (на примере RFC-соединения к манданту 100 системы агента):

- 1) Запустить транзакцию SM59.
- 2) Выбрать пункт меню «Edit» -> «Create».
- 3) В поле «RFC Destination» ввести название RFC-соединения согласно шаблону «ZSBC_<hostname>_<SID>_<mandant>».
- 4) В поле «Connection Type» ввести значение 3.
- 5) На вкладке «Technical Settings» в поле «Target Host» ввести hostname системы агента.
- 6) На вкладке «Technical Settings» в поле «System Number» ввести SID-номер системы агента.
- 7) На вкладке «Logon & Security» в поле «Client» ввести значение рабочего клиента, в котором был пользователь.

- 8) На вкладке «Logon & Security» в поле «User» ввести значение «AGENT».
- 9) На вкладке «Logon & Security» в поле «Password» ввести пароль «Safeerp».
- 10) Выбрать пункты меню «Connection» -> « Save».
- 11) Осуществить проверку созданного RFC-соединения через основное меню «Utilities(M)» -> «Test» -> «Authorization test» или через набор клавиш CTRL+F4 (рис. 47).



Рисунок 47 – Активация проверки RFC-соединения

В случае корректной настройки RFC-соединения появится окно со статусом проверки (рис. 48).

Connection Test AG2	
Connection Type SAP Connection	
Action	Result
Logon	22 msec
Transfer of 0 KB	1 msec
Transfer of 10 KB	2 msec
Transfer of 20 KB	3 msec
Transfer of 30 KB	4 msec

Рисунок 48 – Окно со статусом корректной проверки RFC-соединения

В случае некорректной настройки RFC-соединения появится окно со статусом ошибки (рис. 49).

Connection Type SAP Connection	
Action	Result
Logon	Cancel
Error Details	Name or password is incorrect (repeat logon)

Connection Type SAP Connection	
Action	Result
Logon	Connection Error
Error Details	Error when opening an RFC connection (CPI-CALL: 'ThSAPOCHINIT', communication r
Error Details	ERROR: hostname 'QAS2.sap.loc' unknown
Error Details	LOCATION: SAP-Gateway on host SMM.sap.loc / sapgw00
Error Details	DETAIL: NHLGetNodeAddr: hostname cached as unknown
Error Details	COMPONENT: NI (network interface)
Error Details	COUNTER: 99875
Error Details	MODULE: /bas/749_REL/src/base/ni/niohlcpp
Error Details	LINE: 198
Error Details	RETURN CODE: -2
Error Details	SUBRC: 0
Error Details	RELEASE: 749
Error Details	TIME: Tue Apr 17 11:41:17 2018
Error Details	VERSION: 40

Рисунок 49 – Сообщение о некорректной настройке RFC-соединения

3.3.9. Создание RFC-соединения от сервера управления к Java-агенту

Для создания RFC-соединения от сервера управления к Java-агенту необходимо:

- войти на сервер управления и создать новое RFC-соединение с параметрами, указанными в таблице 4 (рис. 50);
- сохранить соединение;
- осуществить проверку созданного RFC-соединения через основное меню транзакции SM59 «Utilitiles(M)» -> «Test» -> «Connection test» или через набор клавиш CTRL+F3.

Результат корректной настройки RFC-соединения к Java-агенту показан на рис. 51.

RFC Destination AG5_AGENT_SAFEERP

Connection Test Unicode Test 

RFC Destination AG5_AGENT_SAFEERP 

Connection Type T TCP/IP Connection Description

Description

Description 1

Description 2

Description 3

Administration Technical Settings Logon & Security Unicode Special Options

Activation Type

☐ Start on Application Server ☒ Registered Server Program

☐ Start on Explicit Host

☐ Start on Front-End Work Station

Registered Server Program

Program ID SAFEERP_JAVA_AGENT_AG5

Start Type of External Program

☒ Default Gateway Value

☐ Remote Execution

☐ Remote Shell

☐ Secure Shell

CPI-C Timeout

☒ Default Gateway Value

☐ Specify Timeout 60 Defined Value in Seconds

Gateway Options

Gateway Host 10.10.58.36 

Gateway service sapgw00

Рисунок 50 – Настройка RFC-соединения от сервера управления к Java-агенту

Таблица 4 – Значения для параметров RFC-соединения к Java-агенту

Имя параметра	Значение
Program ID	SAFEERP_JAVA_AGENT_<SID>
Gateway Host	<Имя сервера>
Gateway service	<Имя сервиса>

Connection Test AG5_AGENT_SAFEERP	
Connection Type TCP/IP Connection	
Action	Result
Logon	1 msec
Transfer of 0 KB	10 msec
Transfer of 10 KB	11 msec
Transfer of 20 KB	11 msec
Transfer of 30 KB	12 msec

Рисунок 51 – Результат корректной настройки RFC-соединения к Java-агенту

3.3.10. Создание RFC-соединения от сервера управления к ВО-агенту

Для создания RFC-соединения от сервера управления к SAP BO-агенту необходимо выполнить следующие действия на сервере управления ПК «SafeERP Security Suite»:

- 1) Запустить транзакцию SM59.
- 2) Выбрать пункт меню «Edit» -> «Create».
- 3) В поле «RFC Destination» ввести название RFC-соединения.
- 4) В поле «Connection Type» ввести значение «G» (HTTP-связь с внешней системой).
- 5) Нажать кнопку «Сохранить».
- 6) На вкладке «Technical Settings» (рис. 52):
 - в поле «Target Host» ввести имя хоста системы агента;
 - в поле «Service No» ввести номер порта SAP BO;
 - в поле «Path Prefix» ввести значение /SafeERP_BOAgent/.
- 7) На вкладке «Logon & Security» в поле «User» ввести значение «SAFEERPAGENT».
- 8) На вкладке «Logon & Security» в поле «Password» ввести пароль.
- 9) Выбрать пункты меню «Connection» -> «Save».

RFC Destination AG6_BO_AGENT

Connection Test 

RFC Destination AG6_BO_AGENT 

Connection Type G HTTP Connection to External Serv Description

Description

Description 1	
Description 2	
Description 3	

Administration Technical Settings Logon & Security Special Options

Target System Settings

Target Host	10.10.58.37	Service No.	8080
Path Prefix	/SafeERP_BOAgent		

HTTP Proxy Options

Global Configuration

Proxy Host	
Proxy Service	
Proxy User	
Proxy PW Status	is initial

Рисунок 52 – Настройка RFC-соединения к BO-агенту

10) Осуществить проверку созданного RFC-соединения через основное меню транзакции SM59 «Utilitiles(M)» -> «Connection test» или через набор клавиш CTRL+F6.

Результат корректной настройки RFC-соединения к BO-агенту показан на рис. 53.

Connection Test HTTP Destination AG6_BO_AGENT

Destination AG6_BO_AGENT

Ty. HTTP Connection to External Server

Test Result Response Header Fields Response Body Response Text

Detail	Value
Status HTTP Response	200
Status Text	
Duration Test Call	202 ms

Рисунок 53 – Результат корректной настройки RFC-соединения к BO-агенту

3.3.11. Создание RFC-соединения от сервера управления к HANA-агенту

Для создания RFC-соединения от сервера управления к HANA-агенту необходимо:

- войти на сервер управления и создать новое RFC-соединение с параметрами, указанными в таблице 5 (рис. 54, 55);
- сохранить соединение;
- осуществить проверку созданного RFC-соединения через основное меню транзакции SM59 «Utilitiles(M)» -> «Test» -> «Connection test» или через набор клавиш CTRL+F3.

Результат корректной настройки RFC-соединения к HANA-агенту показан на рис. 56.

RFC Destination SAFEERP_HD2_HANA_2_0

Connection Test

RFC Destination **SAFEERP_HD2_HANA_2_0**

Connection Type **G** HTTP Connection to External Serv Description

Description

Description 1	Hana 2.0
Description 2	
Description 3	

Administration **Technical Settings** Logon & Security Special Options

Target System Settings

Host	10.10.58.35	Port	8000
Path Prefix	/_gazis_/SEHA/HANAAgent.xsodata/		

HTTP Proxy Options

Global Configuration

Proxy Host	
Proxy Service	
Proxy User	
Proxy PW Status	is initial

Рисунок 54 – Настройка RFC-соединения от сервера управления к HANA-агенту (вкладка «Technical Settings»)

RFC Destination SAFEERP_HD2_HANA_2_0

Connection Test 

RFC Destination

Connection Type ☒ HTTP Connection to External Serv Description

Description

Description 1

Description 2

Description 3

Administration Technical Settings **Logon & Security** Special Options

Logon Procedure

Logon with User

☐ Do Not Use a User

☒ Basic Authentication

User

PW Status

Logon with Ticket

☒ Do Not Send Logon Ticket

☐ Send Logon Ticket Without Ref. to a Target System

☐ Send Assertion Ticket for Dedicated Target System

System ID Client

Security Options

Status of Secure Protocol

SSL ☒ Inactive ☐ Active

SSL Certificate Cert. List

Authorization for Destination

Рисунок 55 – Настройка RFC-соединения от сервера управления к HANA-агенту (вкладка «Logon & Security»)

Таблица 5 – Значения для параметров RFC-соединения к HANA-агенту

Имя параметра	Значение
Host	<Имя сервера>
Port	<Порт сервера>
Path Prefix	/_gazis_/SEHA/HANAAGent.xsodata/
User	SafeERPagent,
PW Status	Пароль, созданный согласно пункту 3.2.4

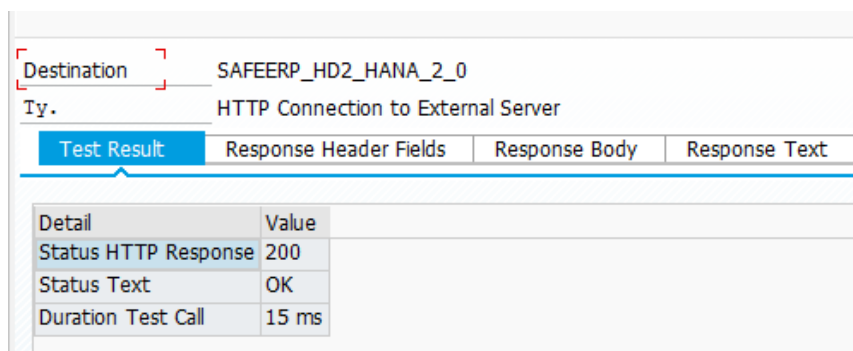


Рисунок 56 – Результат корректной настройки RFC-соединения к HANA-агенту

3.4. Включение ПК «SafeERP Security Suite » в транспортную систему агента

При включении ПК «SafeERP Security Suite» в транспортную систему анализ содержимого транспортных запросов будет проводиться только по сценариям «Безопасность». Для включения ПК в транспортную систему агента необходимо выполнить следующие настройки:

- 1) С помощью транзакции SM59 создать RFC-соединение с системой сервера управления ПК. Выбрать тип соединения 3 (ABAP-соединение).
- 2) Открыть новое окно. Ввести транзакцию SCI. Ввести «Z_SAFEERP» в строке «Name» в разделе «Chek Variant» (рис. 57). Выбрать тип профиля «Global» . Нажать кнопку «Create» .



Рисунок 57 – Создание глобального профиля

- 3) Создать отдельное окно. Ввести транзакцию SCI. Выбрать «Code inspector» -> «Managet of» -> «Test».
- 4) Поставить флаг напротив классов, которые начинаются «/gazis/*» а также «Z*» (рис. 58).

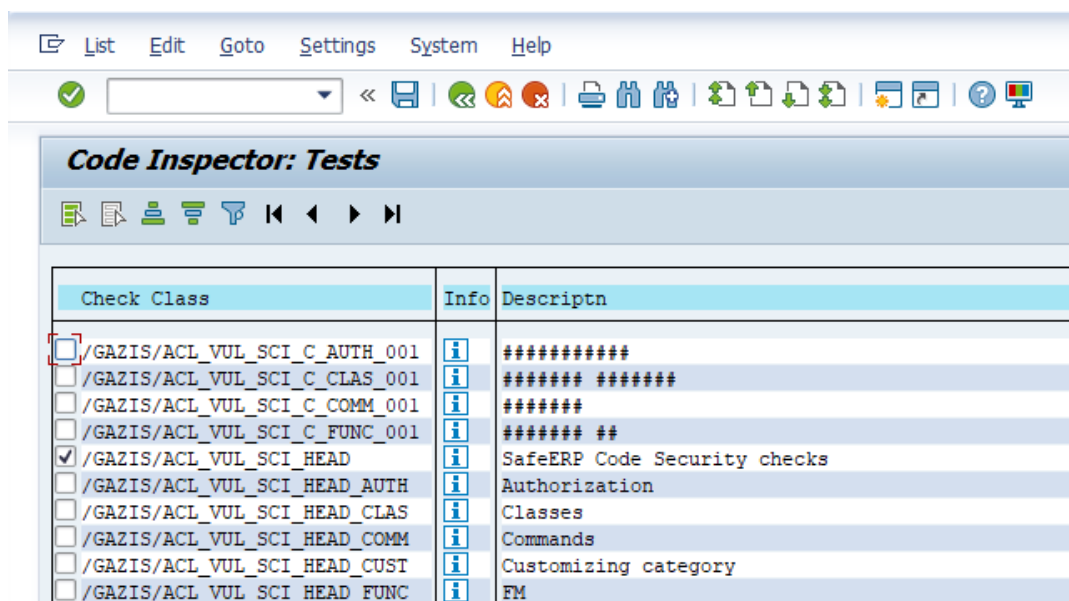


Рисунок 58 – Список классов

- 5) Нажать кнопку . Необходимо подтвердить действия.
- 6) В окне транспортные запросы нажать кнопку .
Примечание – Для сохранения проверок в профиле необходимо ввести название транспортного запроса.
- 7) Вернуться к транзакции SCI.
- 8) Выбрать в меню «Code inspector» -> «Managet of» -> «In reference check system».
- 9) Ввести имя RFC-соединения (рис. 59). Нажать кнопку .

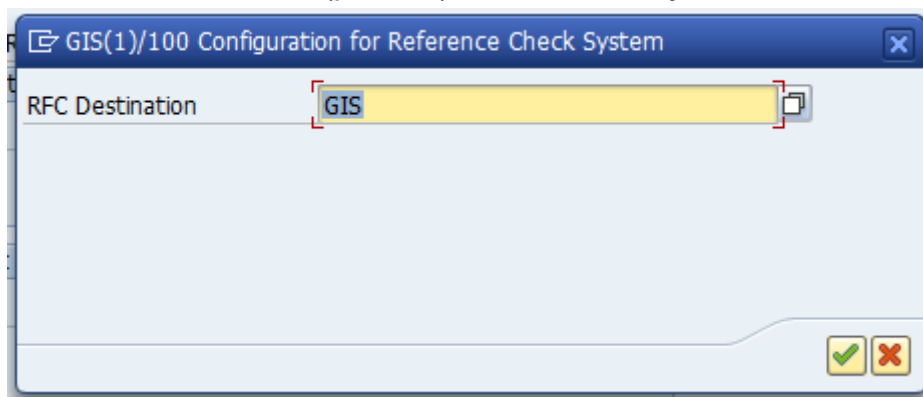


Рисунок 59 – Название RFC соединения

- 10) Вернуться к транзакции SCI. В области «Check Variant» ввести «Z_SAFEERP» (рис. 60), нажать кнопку .

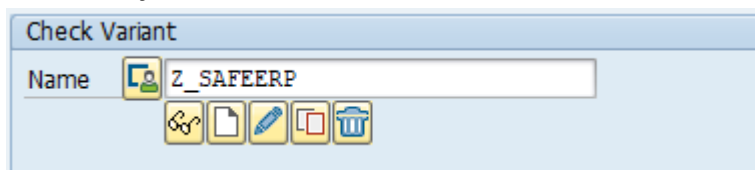


Рисунок 60 – Область «Check variant»

11) Поставить флаг напротив «In reference check system» (рис. 61). Нажать кнопку 

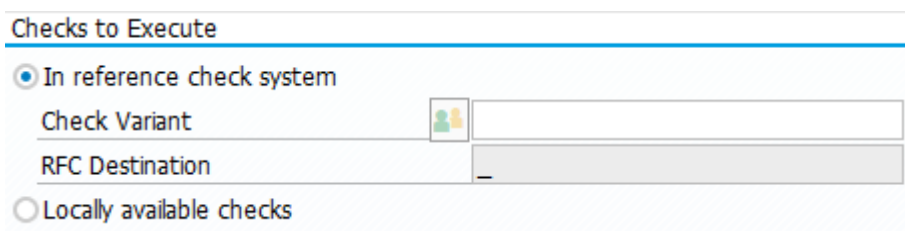


Рисунок 61 – Выбор типа проверок

12) Ввести транзакцию SE11. Ввести «SCICHKV_ALTER» в строке «Database table» (рис. 62), нажать кнопку «Display». В открывшемся окне поставить в меню нажать кнопку .

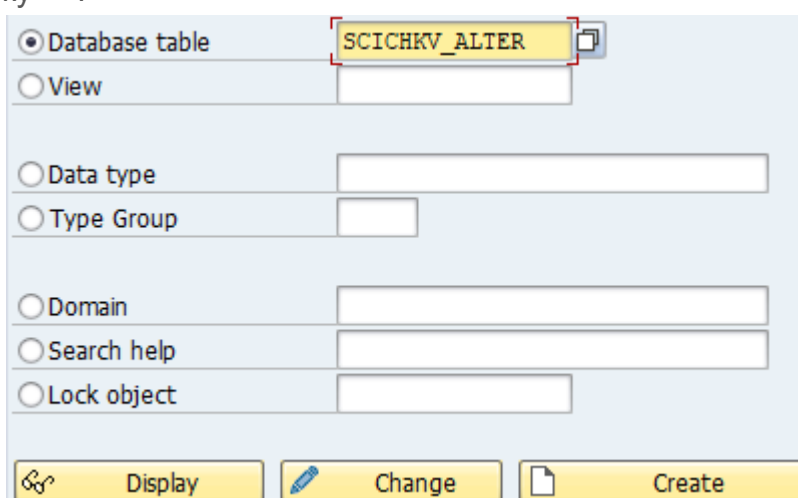


Рисунок 62 – Просмотр таблицы «SCICHKV_ALTER»

Dictionary: Display Table

Transparent Table: SCICHKV_ALTER Active

Short Description: Code Inspector: Mapping Global Check Variant to Alter Ego

Attributes | Delivery and Maintenance | **Fields** | Input Help/Check | Currency/Quantity Fields | Indexes

Field	Key	Ini...	Data element	Data Type	Length	Deci...	Short Description
CHECKVNAME_DEF	☒	☒	SCI_CHKV	CHAR	30	0	Code Inspector: Check Variants
CHECKVNAME_NEW	☐	☐	SCI_CHKV	CHAR	30	0	Code Inspector: Check Variants
RESPONSIBL	☐	☐	RESPONSIBL	CHAR	12	0	Person Responsible for a Repository Object
CREADATE	☐	☐	SCI_UPDDAT	DATS	8	0	Code Inspector: Changed On

Рисунок 63 – Таблица «SCICHKV_ALTER»

13) В открывшемся окне нажать в меню кнопку .

14) В браузере данных таблицы выбрать режим «Изменить» для поля «TRANSPORT» (рис. 64).

Data Browser: Table SCICHKV_ALTER Select Entries 2

Table: SCICHKV_ALTER
Displayed Fields: 4 of 4 Fixed Columns: 1 List Width 0250

CHECKVNAME_DEF	CHECKVNAME_NEW	RESPONSIBL	CREADATE
☐ DEFAULT	Z_SAFEERP_REMOUTE	SAP	05.05.2010
☒ TRANSPORT	Z_SAFEERP_REMOUTE	SAP	05.05.2010

Рисунок 64 – Данные таблицы «SCICHKV_ALTER»

15) В поле «CHECKVNAME NEW» ввести «Z_SAFEERP» (рис. 65).

Table SCICHKV_ALTER Change

CHECKVNAME DEF	TRANSPORT
CHECKVNAME NEW	Z_SAFEERP
RESPONSIBL	SAP
CREADATE	05.05.2010

Рисунок 65 – Ввод данных в таблицу «SCICHKV_ALTER»

16) В транзакции SE03 выбрать пункт «Global Customizing (Transport Organizer)» (рис. 66).

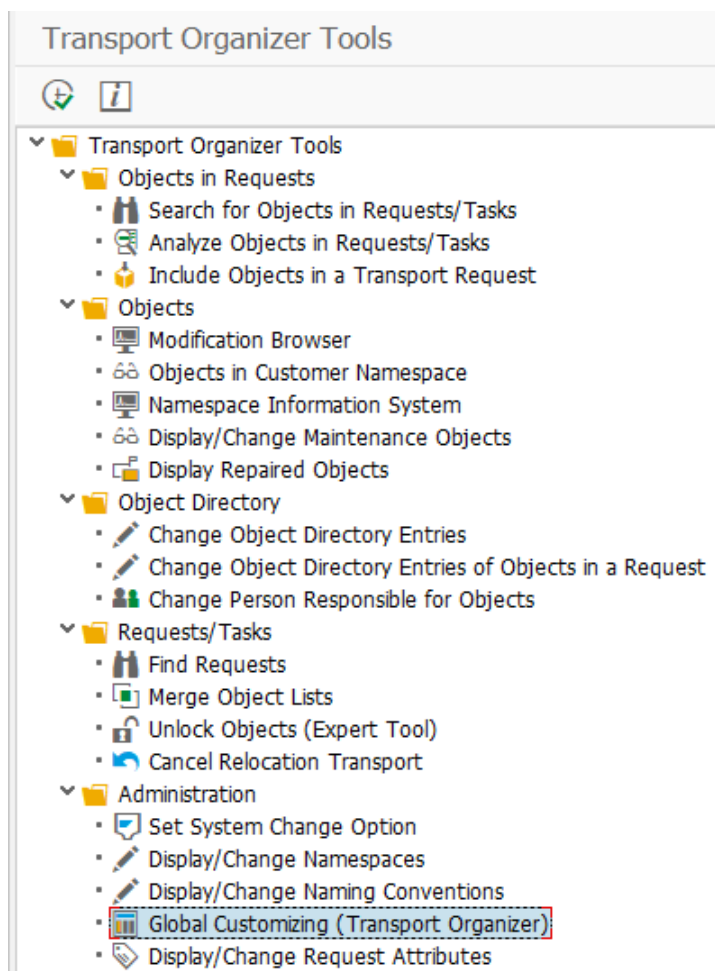


Рисунок 66 – Браузер инструментов организатора переносов

17) В открывшемся окне в поле «Проверки объектов при деблокировании запроса» выбрать нужный вариант (рис. 67):

- globally activated (принудительный запуск проверки);
- globally deactivated (принудительная деактивация проверки);
- set by user (пользователь может включить или выключить проверку).

Global Customizing (Transport Organizer)

Log

Transport error display at logon

☐ globally activated
☐ globally deactivated
☒ Set by User

Object checks at request or task release

☒ globally activated
☐ globally deactivated
☐ Set by User

Object checks (if activated) at release of

☒ Request
☐ Task
☐ Task and Request

Check existence of task documentation at task release

☐ globally activated
☐ globally deactivated
☒ Set by User

Request Release

☐ Release in Background Only
Server for Background Release

Рисунок 67 – Окно организатора переносов глобальной настройки

При начальных установках SAP-системы существует возможность игнорировать результаты проверки (например, ошибки или уязвимости в коде) и деблокировать транспортный запрос. Чтобы отключить эту возможность, необходимо через транзакцию SM30 для таблицы (ракурса) TRCHECK (рис. 68) установить в параметре «SLIN» значение «Check active, error preventing release» (рис. 69).

Maintain Table Views: Initial Screen

Find Maintenance Dialog

Table/View

Restrict Data Range

☒ No Restrictions
☐ Enter conditions
☐ Variant

Display Maintain Transport Customizing

Рисунок 68 – Таблица TRCHECK

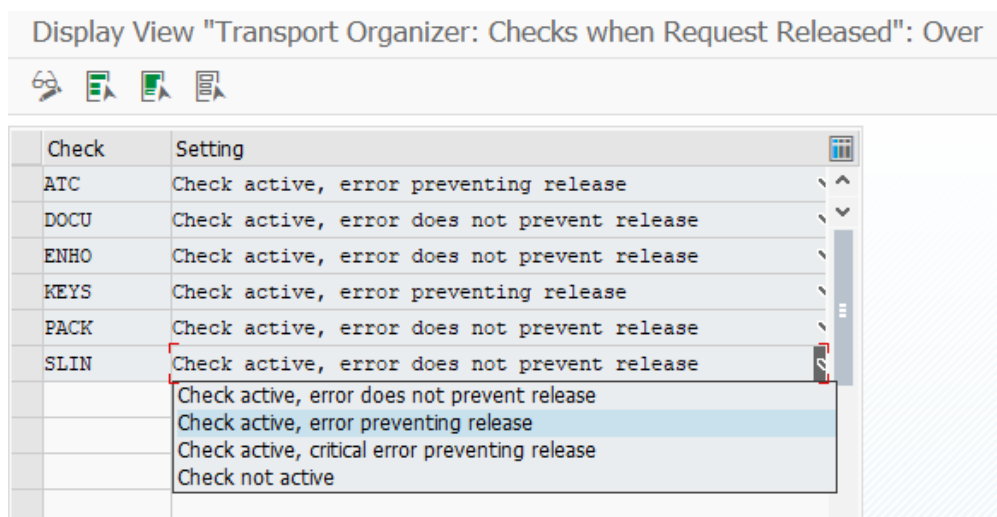


Рисунок 69 – Проверки при деблокировании запросов в организаторе переносов глобальной настройки

3.5. Включение ПК «SafeERP Security Suite» в систему проверки кода

Для включения ПК «SafeERP Security Suite», как основного программного модуля (по умолчанию), в систему проверки кода прикладного программного обеспечения SAP необходимо выполнить следующие настройки:

- 1) Ввести транзакцию SE11. Ввести «SCICHKV_ALTER» в строке «Database table» (рис. 62), нажать кнопку «Display». В открывшемся окне поставить в меню нажать кнопку  (рис. 63).
- 2) В браузере данных таблицы выбрать режим  «Изменить» для поля «DEFAULT» (рис. 70).

Data Browser: Table SCICHKV_ALTER Select Entries 2			
     			
Table: SCICHKV_ALTER			
Displayed Fields: 4 of 4		Fixed Columns: 1	List Width 0250
CHECKVNAME_DEF	CHECKVNAME_NEW	RESPONSIBL	CREADATE
☒ DEFAULT	Z_SAFEERP_REMOUTE	SAP	05.05.2010
☐ TRANSPORT	Z_SAFEERP_REMOUTE	SAP	05.05.2010

Рисунок 70 – Данные таблицы «SCICHKV_ALTER»

- 3) В поле «CHECKVNAME NEW» ввести «Z_SAFEERP» (рис. 71).

CHECKVNAME DEF	DEFAULT
CHECKVNAME NEW	Z_SAFEERP
RESPONSIBL	SAP
CREADATE	05.05.2010

Рисунок 71 – Ввод данных в таблицу «SCICHKV_ALTER»

Установка данных настроек позволит вызывать по умолчанию сценарии проверок ПК «SafeERP Security Suite» для анализа кода выбранной программы. В транзакции SE80 ПК «SafeERP Security Suite» будет запускаться через стандартный путь вызова инспектора кода (рис. 72).

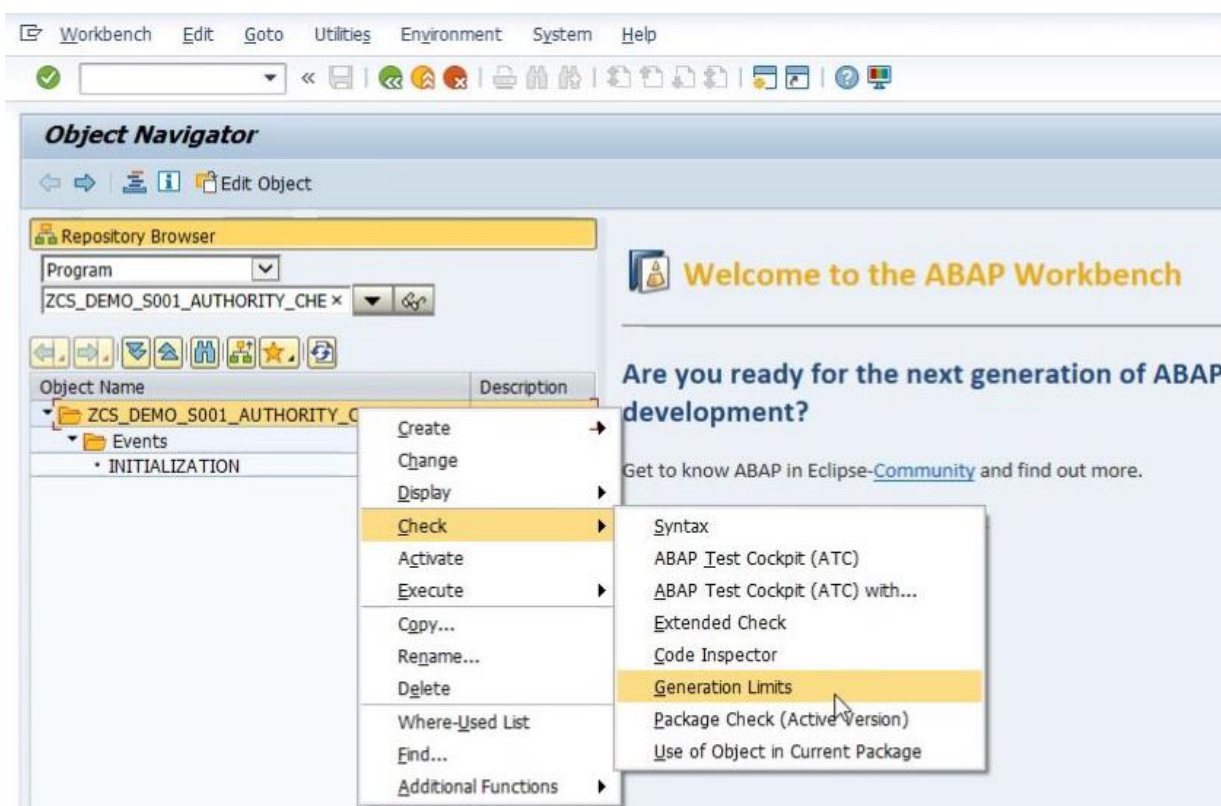


Рисунок 72 – Навигатор по объектам

Далее для выбранной программы по умолчанию применяются проверки ПК «SafeERP Security Suite» по сценариям безопасности (рис. 73).

Code Inspector: Results for ZCS_DEMO_S001_AUTHORITY_CHECK (PROG)					
Code Inspector					
Code Inspector					
	D..	...	E..	Checks	Error
▼				List of Checks	1
▼				SafeERP Code Security checks (Remote)	1
▼				Security category	1
▶				Alias authorization in AUTHORITY-CHECK	1
•				Alias authorization in SUBMIT report	0
•				All occurrences of sy-sysid	0
▶				All occurrences of sy-uname	0
•				Broken AUTHORITY-CHECKs	0
•				Exposed kernel calls	0
•				Exposed system calls	0
•				Hard-coded OS checks (SY-OPSYs)	0
•				Hard-coded SAP client checks (SY-MANDT)	0
•				Hard-coded SAP host checks (SY-HOST)	0
•				Hard-coded SAP SID checks (SY-SYSID)	0
•				Hard-coded system date checks (SY-DATUM)	0
•				Outgoing ftp connections	0
•				OS command execution (client OS)	0
•				Dangerous kernel call (` C_REMOVE`)	0
•				ABAP command injection (PROGRAM)	0
•				ABAP command injection (REPORT)	0

Рисунок 73 – Результаты проверки ПК «SafeERP Security Suite»

4. Удаление ПК «SafeERP Security Suite»

При необходимости удалить ПК «SafeERP Security Suite» с системы агента важно учитывать следующие условия:

- при выполнении действий по полному удалению ПК «SafeERP Security Suite» все программные модули ПК будут удалены с системы агента (при необходимости блокирования доступа к одному из модулей ПК возможна только деактивация полномочий к определенному функционалу);
- для сохранения возможности удаления компонентов ПК «SafeERP Security Suite» с системы агента запрещается использовать для работы объекты из установленных ПК с названиями, начинающимися с «/GAZIS/» (разрабатывать сторонние объекты с именами «/GAZIS/*»).

Полное удаление ПК «SafeERP Security Suite» с системы агента можно заменить его деактивацией, например, произвести удаление только компонентов ПК в соответствии с подразделом 4.2.

4.1. Удаление ПК «SafeERP Security Suite »

Для полного удаления ПК «SafeERP Security Suite» с сервера управления необходимо выполнить следующие настройки:

- 1) Запустить транзакцию SAINT в манданте системы 000 (рис. 74).

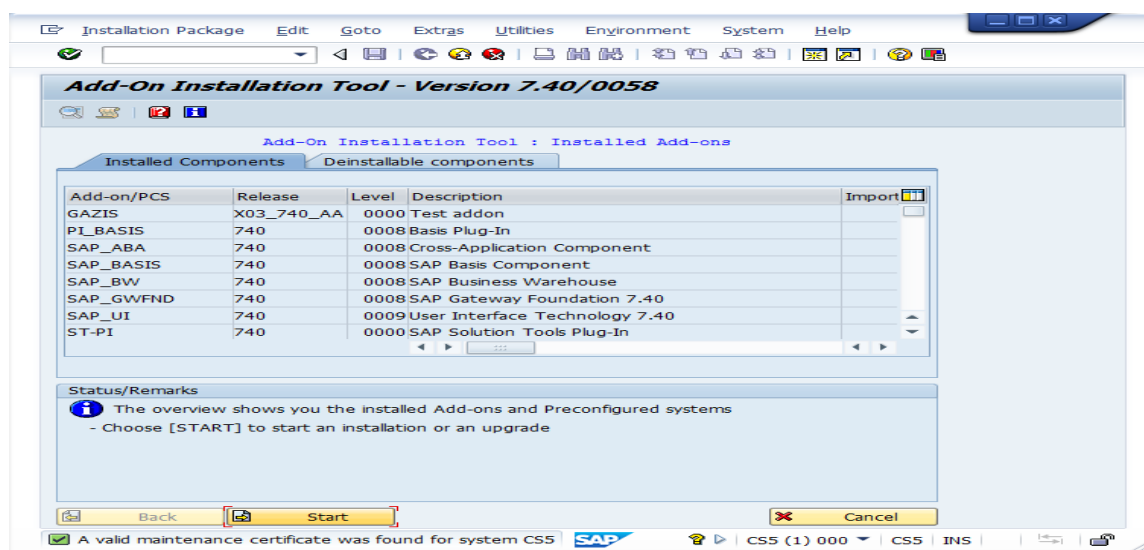


Рисунок 74 – Запуск транзакции SAINT

- 2) Перейти на вкладку «Deinstallable components» (рис. 75).

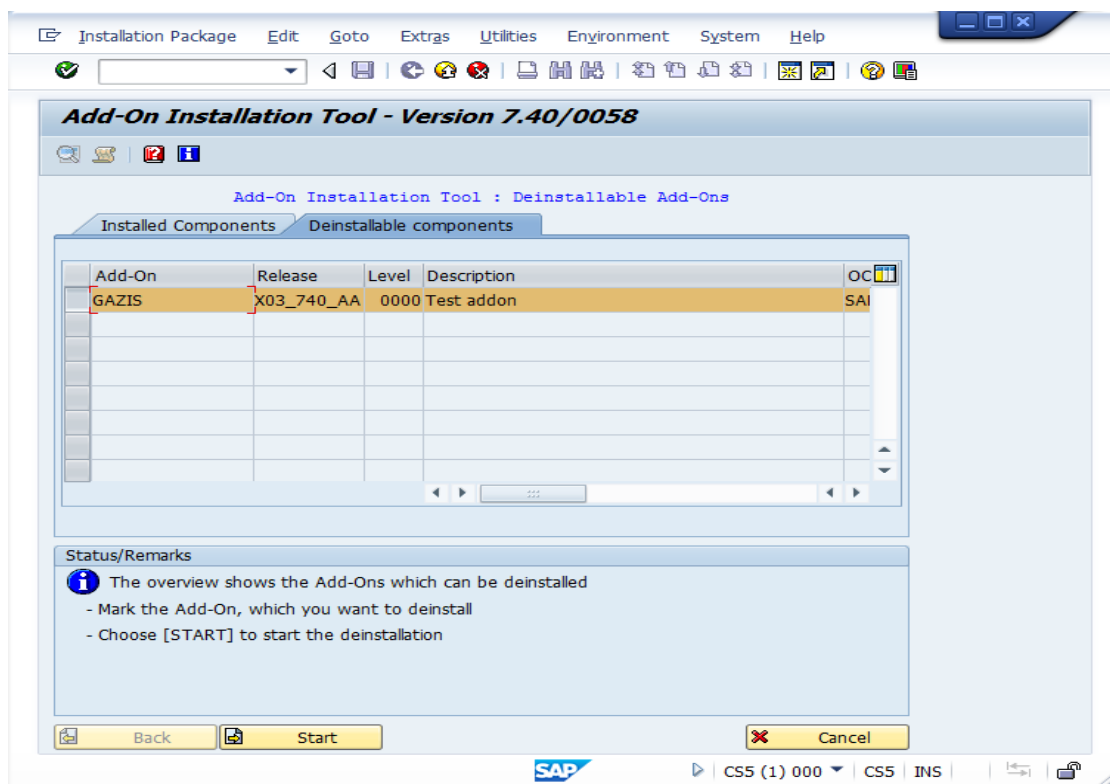


Рисунок 75 – Вкладка «Deinstallable components»

- 3) Выбрать в столбце «Add-On» значение «GAZIS», нажать кнопку «Start». В появившемся окне нажать кнопку  (рис. 76).

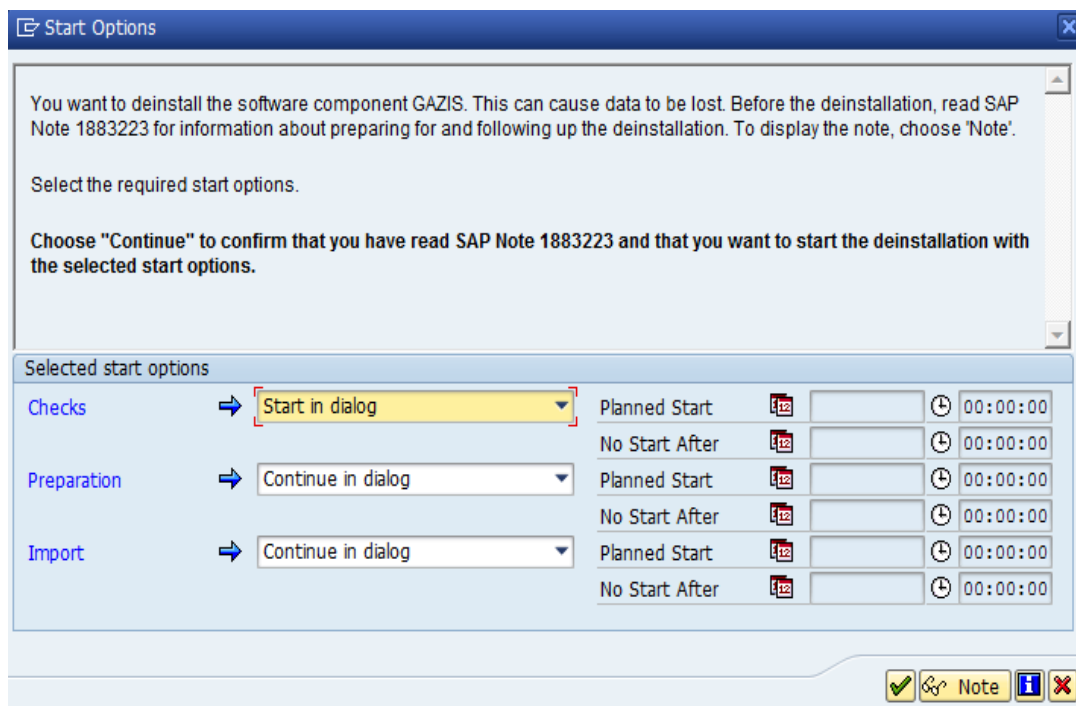


Рисунок 76 – Удаление ПК «SafeERP Security Suite»

- 4) Дождаться успешного окончания процесса удаления (рис. 77).

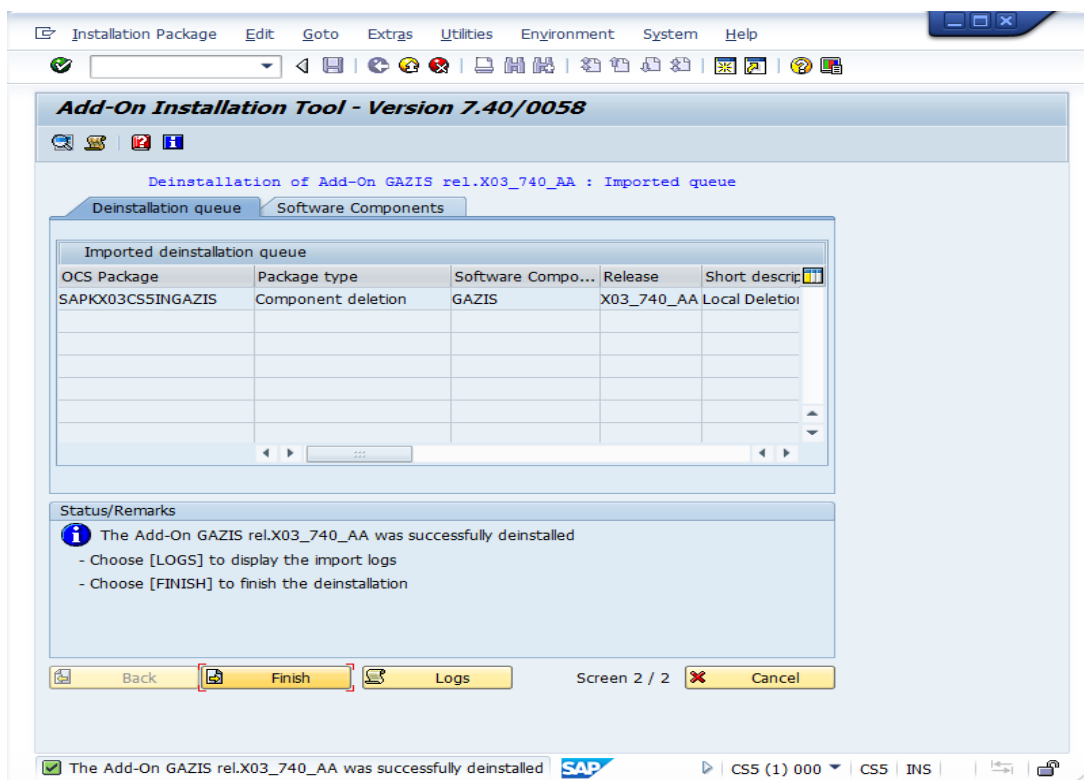


Рисунок 77 – Информационное сообщение об удалении ПК «SafeERP Security Suite»

5) Нажать кнопку «Finish».

4.2. Удаление компонентов ПК «SafeERP Security Suite»

Если есть необходимость только в деактивации работы комплекса, а не в полном его удалении с систем, можно произвести удаление RFC-соединений между системами или удалить учетные записи с полномочиями на работу с ПК.

4.2.1. Удаление RFC-соединений

Для удаления RFC-соединений в рабочем мандате SAP-системы сервера управления ПК «SafeERP Security Suite» необходимо зайти под учетной записью администратора системы, запустить транзакцию SM59 и удалить RFC-соединения, созданные для ПК «SafeERP Security Suite».

4.2.2. Удаление учетных записей

Для удаления учетных записей в рабочем мандате SAP-системы агента необходимо зайти под учетной записью администратора системы и запустить транзакцию SU01, удалить пользователей, созданных для функционирования RFC-соединений для ПК «SafeERP Security Suite».

При необходимости удаления учетных записей в рабочем мандате SAP-системы сервера управления ПК «SafeERP Security Suite» требуется зайти под учетной записью администратора системы и запустить транзакцию SU01, удалить пользователей, созданных для работы с ПК «SafeERP Security Suite», либо удалить назначенные для использования ПК «SafeERP Security Suite» роли и профили.

4.2.3. Удаление АВАР-агента

Для полного удаления АВАР-агента необходимо выполнить следующие настройки:

- 1) Запустить транзакцию SAINT в манданте системы 000 (рис. 78).

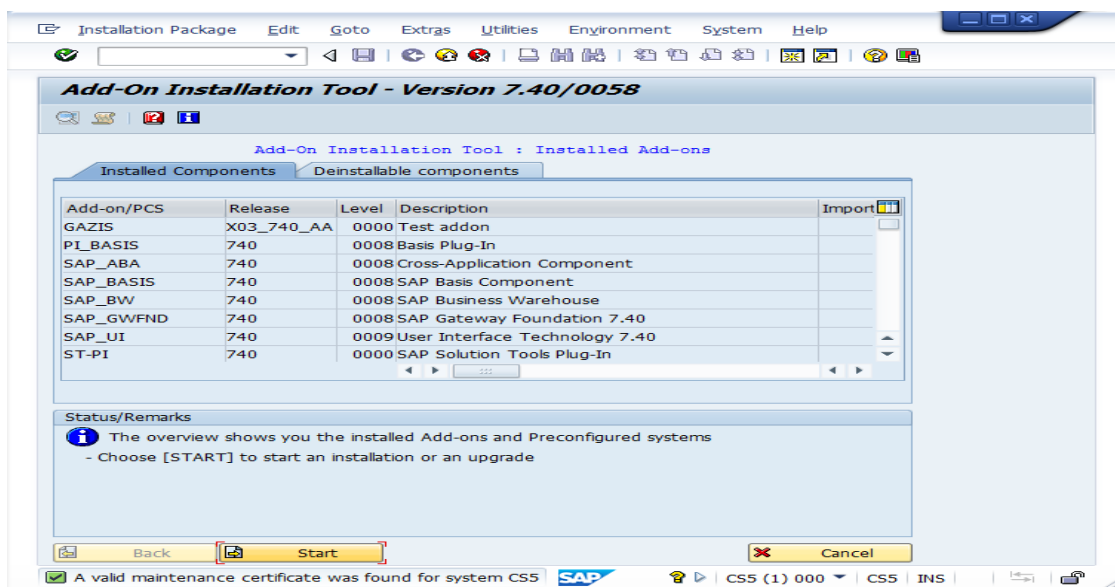


Рисунок 78 – Запуск транзакции SAINT

- 2) Перейти на вкладку «Deinstallable components» (рис. 79).

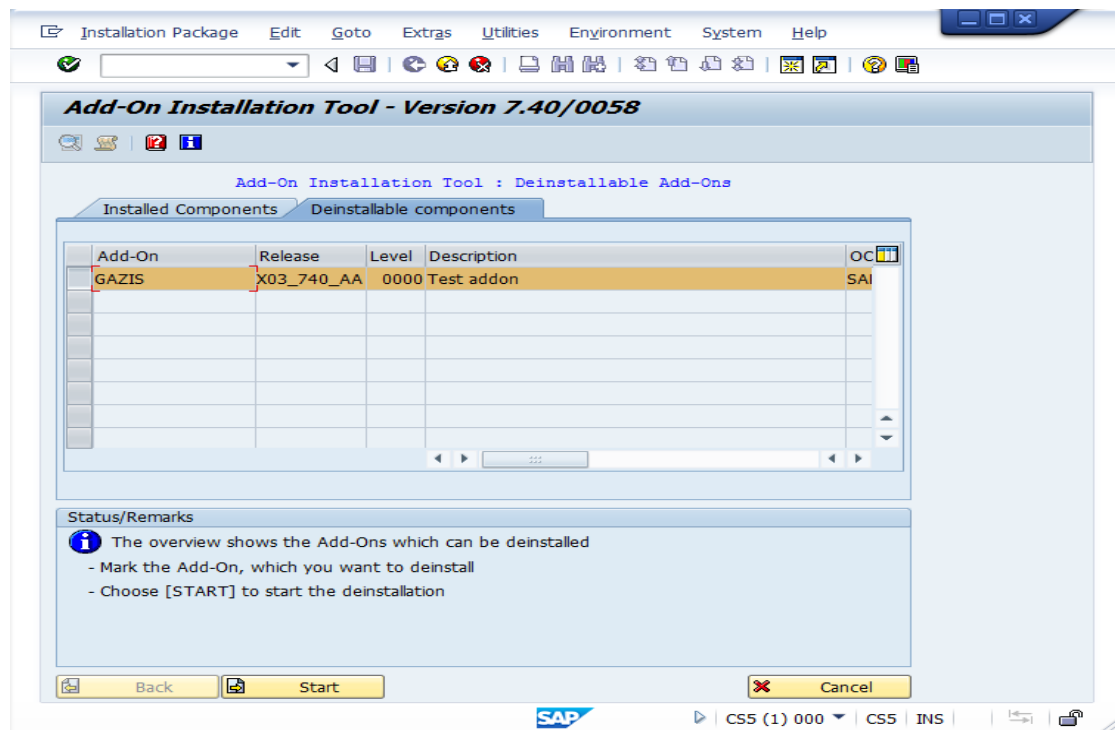


Рисунок 79 – Вкладка «Deinstallable components»

- 3) Выбрать в столбце «Add-On» значение «GAZIS», нажать кнопку «Start». В появившемся окне нажать кнопку  (рис. 80).

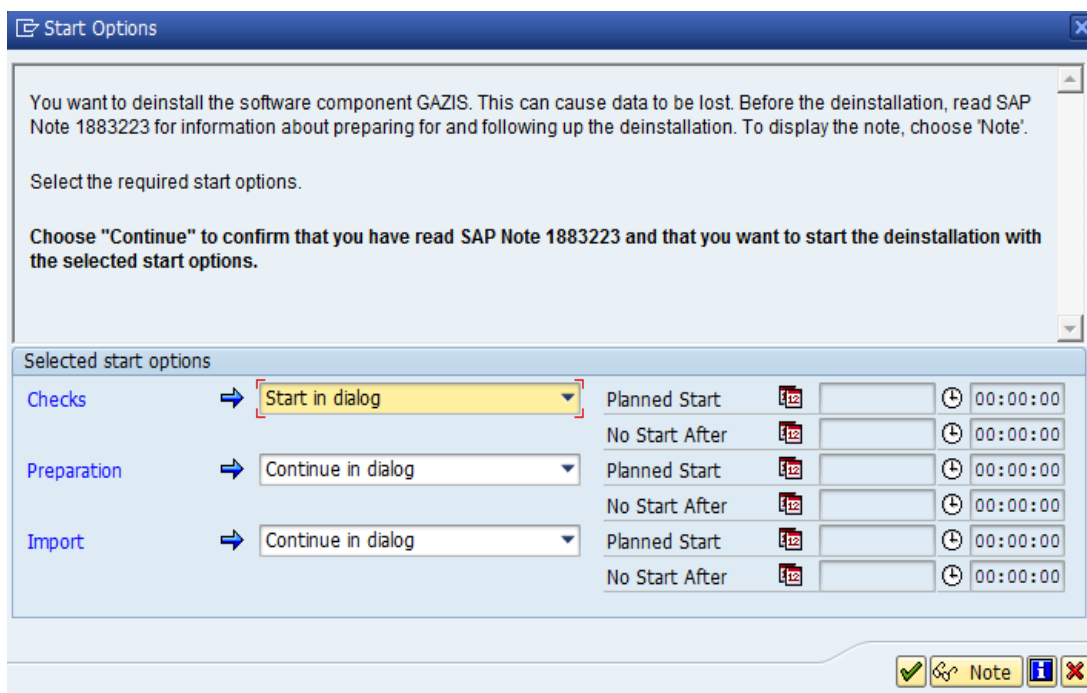


Рисунок 80 – Деактивация агента

4) Дождаться успешного окончания процесса удаления (рис. 81).

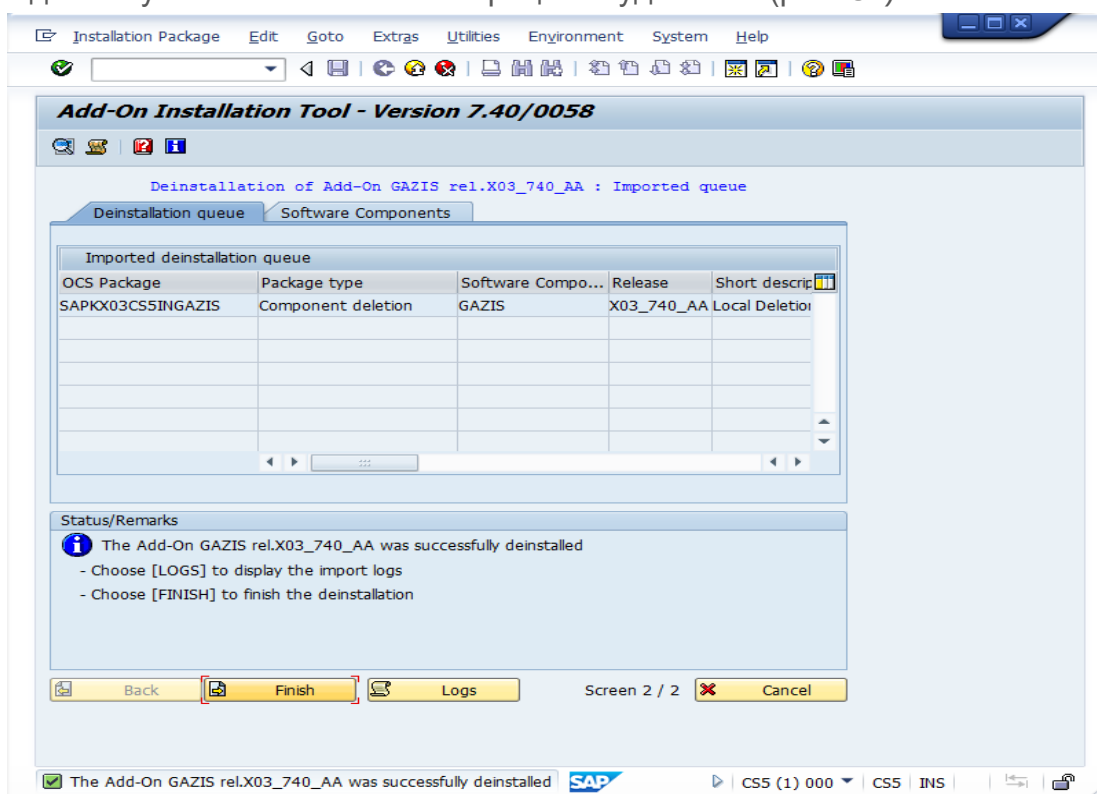


Рисунок 81 – Сообщение о деактивации агента

5) Нажать кнопку «Finish».

4.2.4. Удаление Java-агента

Для удаления Java-агента необходимо запустить соединение с сервером приложения

```
MIS - PuTTY
```

```
*****  
*****  
*****#####*****  
*****#####*****  
*****#####*****  
*****#####*****  
*****#####*****  
*****#####*****  
*****#####*****  
*****#####*****  
*****#####*****  
*****#####*****  
  
Telnet Administration  
SAP Java EE Application Server v7.40  
  
User name: Administrator  
Password:  
  
Welcome to server node 2556050.  
  
>
```

Далее следует выполнить команду «undeploy vendor=gazis.com name=safeerp_java_agent~ear». Результатом успешного удаления агента будет сообщение: «[Success]: gazis.com safeerp java agent~ear» (рис. 83).

```

type: [SDA], name: [safeerp_java_agent~ear], vendor: [gazis.com], location: [
GazISDevelopment], version: [20161027142635], status: [Success], description: []

===== END UNDEPLOY RESULT =====

===== Summary - Undeploy Result - Start =====
-----
Type | Status   : Count
-----
> SCA(s)
> SDA(s)
  - [Success] : [1]
-----

Type | Status   : Id
-----
> SCA(s)
> SDA(s)
  - [Success] : gazis.com_safeerp_java_agent~ear,
-----

===== Summary - Undeploy Result - End =====

>

```

Для удаления ВО-агента необходимо в браузере выполнить вход в приложение «Manager App» на веб-сервере TomCat, для этого в адресной строке набрать «имя сервера SAPBO»: «порт TomCAT»//manager/html», например: «<http://agn.sap.loc:8080/manager/html>». Ввести логин и пароль, созданный в перечислении 1 пункта 3.1.3. В разделе «Application» найти приложение /SafeERP BOAgent, нажать кнопку «Undeploy».

4.2.6. Удаление HANA-агента

Для удаления HANA-агента необходимо запустить приложение «SAP HANA Studio», выполнить соединение с системой SAP HANA, из которой предполагается удаление агента:

- 1) Выбрать пункты меню «Lifecycle Management» -> «Application Lifecycle Management» -> «Home» (рис. 84), в появившемся окне выбрать учётные данные пользователя с полномочиями (sap.hana.xs.lm.roles::Administrator) (рис. 85).

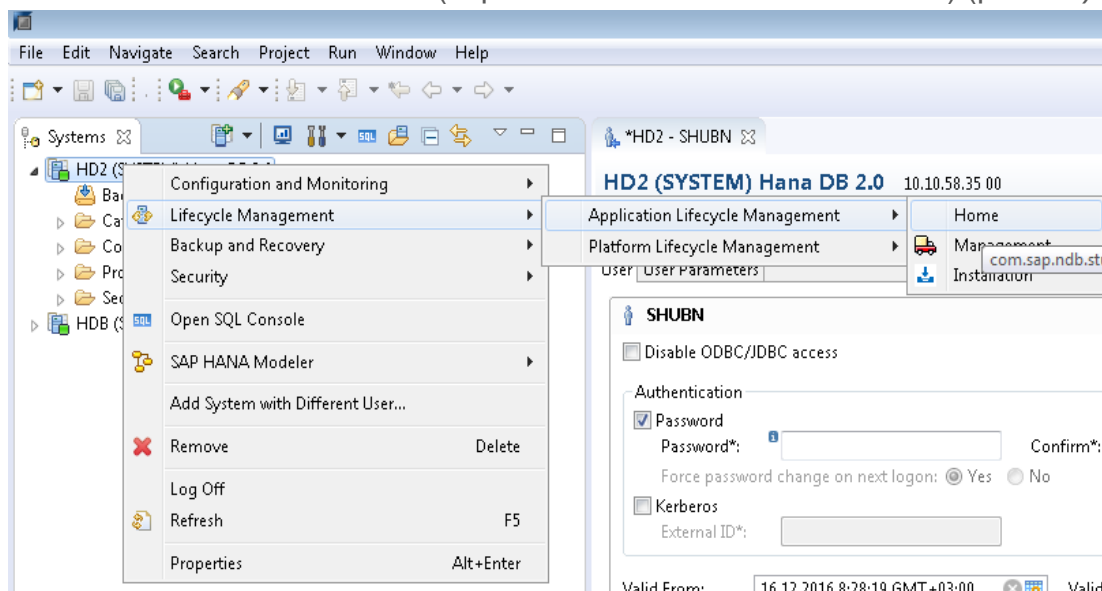


Рисунок 84 – Внешний вид SAP HANA Studio

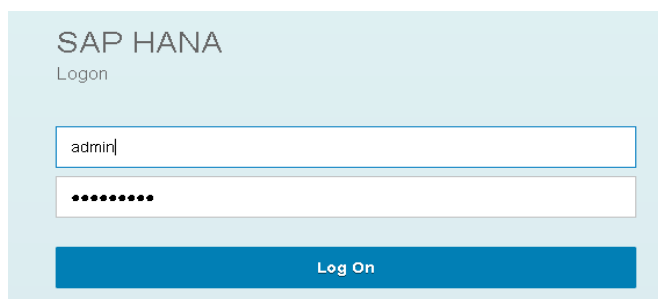


Рисунок 85 – Окно авторизации в «Application Lifecycle Management»

- 2) В появившемся окне выбрать раздел «Delivery Units» (рис. 86).

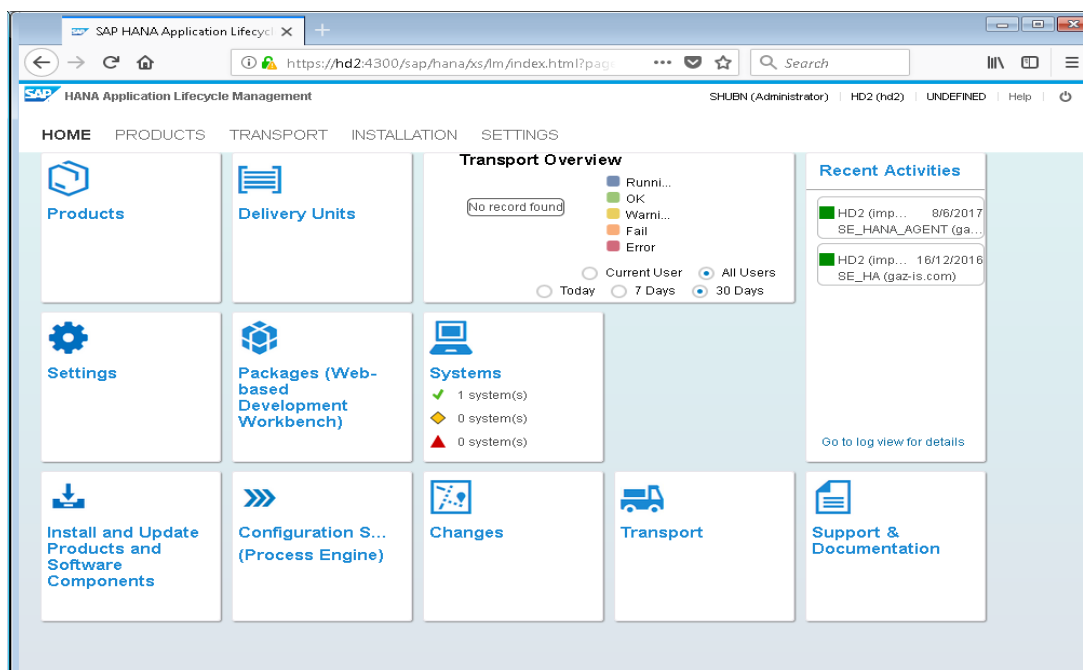


Рисунок 86 – Интерфейс «Application Lifecycle Management»

- 3) Для удаления приложения HANA-агента с системы необходимо выбрать строку с установленным компонентом ПК «SafeERP Security Suite», нажать кнопку «Delete», в появившемся окне выделить пункт «including objects and packages» и нажать кнопку «Yes» (рис. 87).

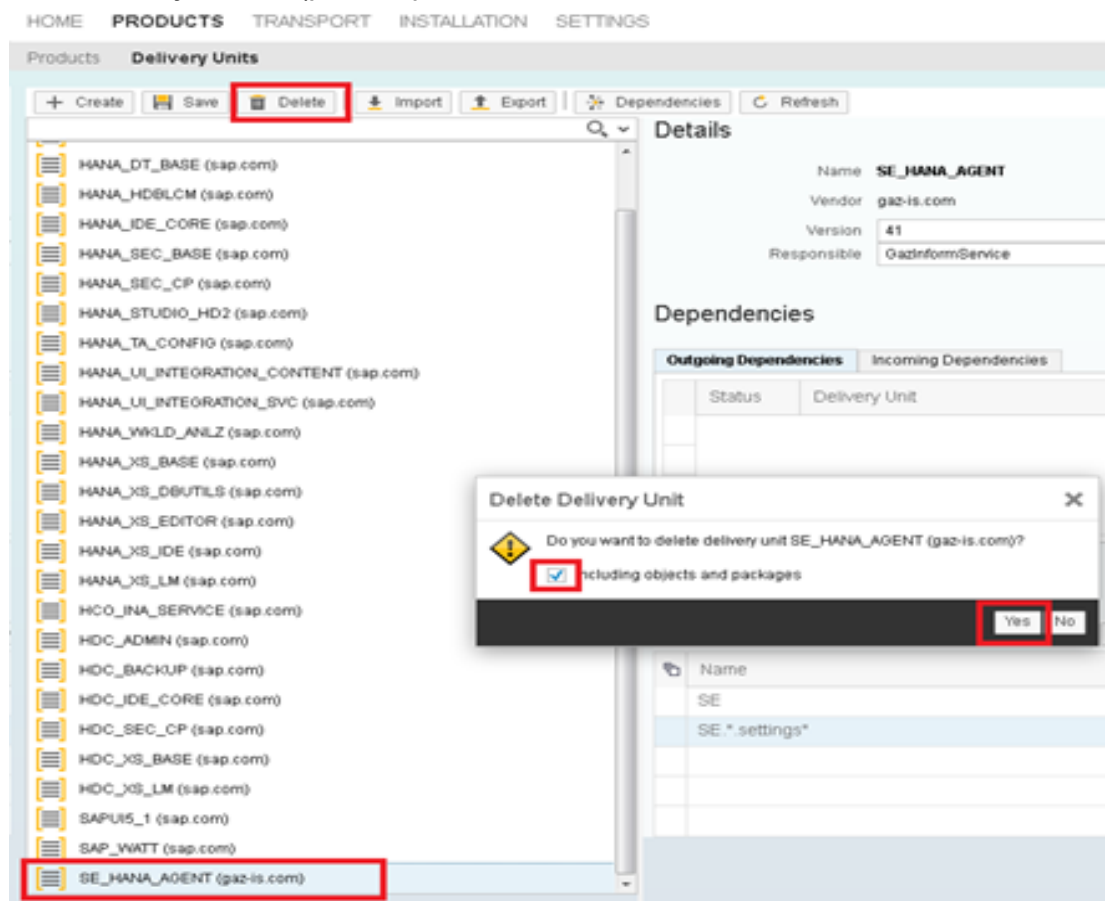


Рисунок 87 – Интерфейс удаления HANA-агента

- 4) В появившемся окне (рис. 88) активировать удаление, нажав кнопку «Yes».

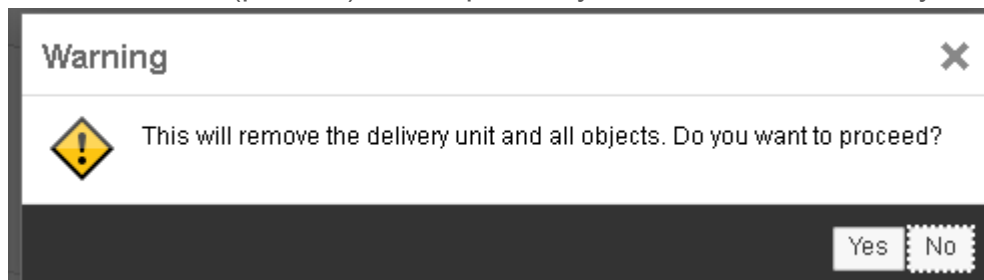


Рисунок 88 – Удаление HANA-агента

5. Сообщения системному программисту

Сообщения системному программисту, которые могут возникать в процессе установки ПК, перечислены в разделе 3.

Сообщения системному программисту, которые могут возникать при удалении компонентов ПК, входят в стандартный SAP-функционал указанных транзакций (SM59 и SU01) и не рассматриваются в данном руководстве.