This connector is no longer supported by Oracle.

**Oracle® Enterprise Single Sign-on
Provisioning Gateway**

CONTROL-SA Integration and Installation Guide

Release 1%1.%1.0

E1) +$%01

March 2010

ORACLE®

Oracle Enterprise Single Sign-on Provisioning Gateway CONTROL-SA Integration and Installation Guide, Release 11.1.1.1.0

E15701-01

Table of Contents

About CONTROL-SA

CONTROL-SA is BMC Software's solution that enables management of security systems distributed across multiple incompatible platforms. This document describes how to use this solution in your own applications.

Audience

This guide is intended for administrators who either install or configure the USA-APIs for CONTROL-SA. This guide describes concepts and tools required by the administrator for setting up and administering the CONTROL-SA Connector.

Users of this guide should have knowledge of the following:

- CONTROL-SA Functionality
- CONTROL-SA ESS Server configuration
- CONTROL-SA Agent
- Functioning of USA-API

Acronym or Abbreviation	Full Name
SSO Agent	ESSO-LM Agent
SSO Administrative Console	ESSO-LM Administrative Console
ESSO-LM	Oracle Enterprise Single Sign-On Logon Manager
ESSO-AM	Oracle Enterprise Single Sign-On Authentication Manager
ESSO-KM	Oracle Enterprise Single Sign-On Kiosk Manager
ESSO-PG	Oracle Enterprise Single Sign-On Provisioning Gateway
ESSO-PR	Oracle Enterprise Single Sign-On Password Reset
SSO	ESSO-LM
FTU	First Time Use
SSO Agent	ESSO-LM Agent

CONTROL-SA

USA-API stands for Universal Security Administration Application Programming Interface. The USA-API is the interface between a Resident Security System (referred to as the RSS) and SA-Agent.

CONTROL-SA includes the components illustrated below, which together provide centralized security administration for the entire enterprise.
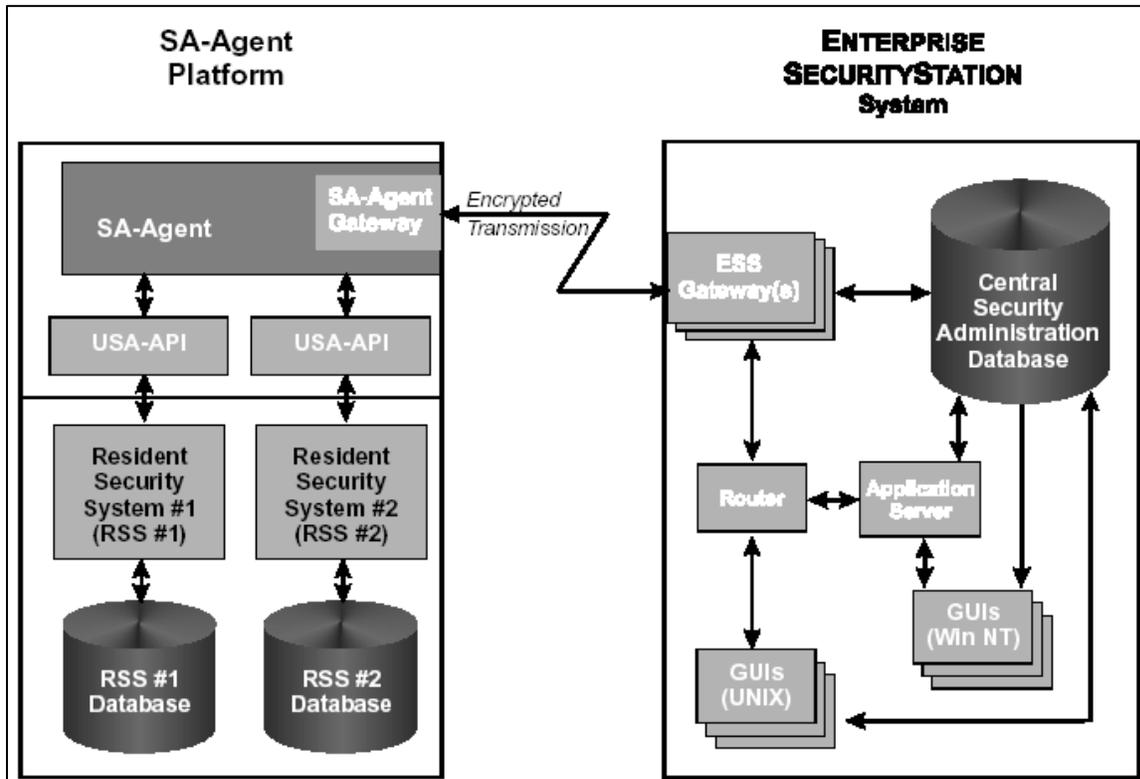
The SA-Agent platform contains the following elements:

One or multiple instances of the SA-Agent program. This program receives commands from ENTERPRISE SECURITY STATION and passes them to the correct USA-API. Messages from the USA-API are passed via SA-Agent to ENTERPRISE SECURITY STATION.

SA-Agent contains the SA-Agent gateway. Using a TCP/IP or an SNA LU6.2 link, this module connects the SA-Agent platform to the ENTERPRISE SECURITY STATION workstation and enables communication.

One or more USA-APIs. Each USA-API is an interface that is designed to communicate with a specific type of RSS.

The Resident Security System (RSS) is a security product or module. The RSS can be the native security of an operating system (for example, Solaris, HP-UX, Novell NetWare) or any other product that implements security (for example, RACF, Sybase, SeOS). While the RSS can reside anywhere in the network, it is managed via the SA-Agent platform. Each RSS has its own RSS database containing security administration data for the RSS.

Interaction between the SA-Agent and the RSS is achieved through the USA-API. Since each RSS has different facilities and operates using its own unique terminology, SA-Agent is provided with a dedicated USA-API for each type of RSS supported. The use of dedicated USA-APIs enables SA-Agent to handle the unique features and operations of each RSS.

USA-API works as a communicator between CONTROL-SA and the Resident Security System (RSS). It takes inputs from CONTROL-SA and formats them into messages that are understood by ESSO-PG. In turn, it interprets the results from ESSO-PG and formats the results into a form that is understood by CONTROL-SA.

USA–API interacts with ESSO-PG using the CLI provided by Passlogix and the user file, which has the user information.

The CONTROL-SA Connector manages the following:

- Entities. Users, User-to-User Group Connections (Credentials)
- Attributes. These are keywords related to User, User Group, and User-to-User Group Connections.

CONTROL-SA Connector Architecture

The CONTROL-SA Connector is designed to manage the ESSO-PG repository and is configured on a W2K platform with CONTROL-SA Agent for W2K installed.

Interface

The following explains the communication mechanism between USA-API and SA-Agent and USA-API and ESSO-PG.

Interface with the SA-Agent

USA–API receives the inputs as function parameters from SA-Agent. Results are returned as return values from functions. Additional values are updated into the addresses passed as function parameters. Refer Chapter 13 of the *USA-API Design and Implementation Guide* for more details which explains all data types, which are used between SA-Agent and USA-APIs.

Interface with ESSO-PG repository

The Get functions for User Group and User to User Group Connection and the Set functions of the CONTROL-SA Connector application are implemented using the CLI provided by ESSO-PG and the Get function for Users has been implemented using the user file, which has the user information.

Installation Overview

This provides required information and step-by-step instructions for installing the CONTROL-SA Connector.

Before running the installation procedure, it is recommended that you review the information in this section to ensure that the installation procedure runs smoothly and successfully.

System Requirements

Installing and operating CONTROL-SA Connector requires the following:

Operating System	Windows 2000 Server
Software	Oracle ESSO-PG
Memory	256 MB RAM
Disk Space	10 MB free disk space (preferably in the local drive)
Installation Device	CD-ROM drive

Pre-installation Checks

Perform the following steps before installing the Connector:

1. Determine the name of the RSS to be managed by the CONTROL-SA Connector as mentioned in the ESS GUI RSS Window.
2. Default admin should be a dummy account and it should be added through ESS GUI.

Installation Steps

Installation of the CONTROL-SA Connector consists of the following steps:

1. Install new RSS Type
2. Install Of CONTROL-SA Module
3. Configure CONTROL-SA Module
4. Apply the Patch to Support Additional Java Class PATH in the CONTROL-SA Agent
5. Copy the ASCII flat file containing ESSO-PG PM users

RSS parameters must be configured for each RSS to be managed via the SA-Agent platform.

Installation Instructions

This section describes how to install the CONTROL-SA Connector and integrate it into the SIM workflow.

Installation of new RSS Type

The CONTROL-SA Agent for the Passlogix package contains a file:

```
ManagedSystem_Passlogix.sh
```

This script adds support for your Managed System type in Enterprise SecurityStation. It is used in defining the new Managed System Type Entity and the new user-defined Keywords in the ESS database.

To import a new Managed System type and keywords into ESS, or to modify existing Keywords:

1. Log in to the Enterprise SecurityStation workstation as the ESS owner.

2. Copy the script **ManagedSystem_Passlogix.sh** from the deployment module directory (`\Program Files\EagleEye\SA-Agent\DATA\USAAPI\Passlogix`) to the ESS home directory.

3. Enter the following command to change the file permissions and change to a tcsh shell:
   ```
   chmod 500 ManagedSystem_Passlogix.sh
   tcsh
   ```

4. Run the **ManagedSystem_Passlogix.sh** script. You are requested to provide the name and password for an ESS administrator.

5. Enter the name and password of an ESS administrator who has sufficient access rights to modify Managed System and ESS keywords information in Enterprise SecurityStation.

6. On a Microsoft Windows computer where ESS Console is installed:

   a. From the Start menu, select **Programs** > **Enterprise SecurityStation** > **Managed System Type Activation**. The Login dialog box opens.

   b. Specify the ESS log in name and password of an ESS administrator who is defined as a Superuser. Select the relevant Enterprise SecurityStation Login Profile. Click **OK**.

      The Managed System Type Activation window opens:
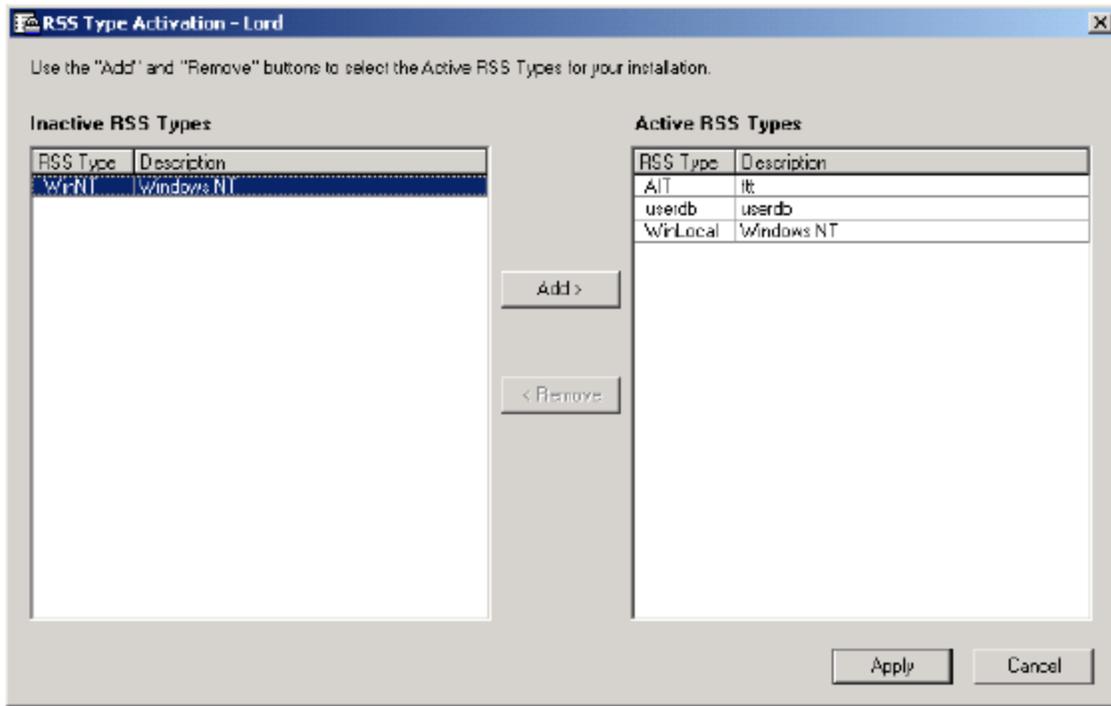
c. Verify that the new Managed System type appears in the **Active Managed System Types** list.

d. Click **Apply** to save your changes to the Enterprise Security Station database. The window remains open while the changes are saved. The process of saving the changes to the database might require several minutes. Upon completion, a message box is displayed, reminding you to stop and restart Orbix, Gateway, and ESS Console processes.

e. Click **OK** to close the message box.

f. Click **Done** to close the window.

Installation of CONTROL-SA Module

1. Log in to the machine and insert the CD into the CD-ROM drive.

2. Double-click the `setup.exe` file, which will be available on subdirectory `Setup/win`.

3. Click **Next** to start the installation.
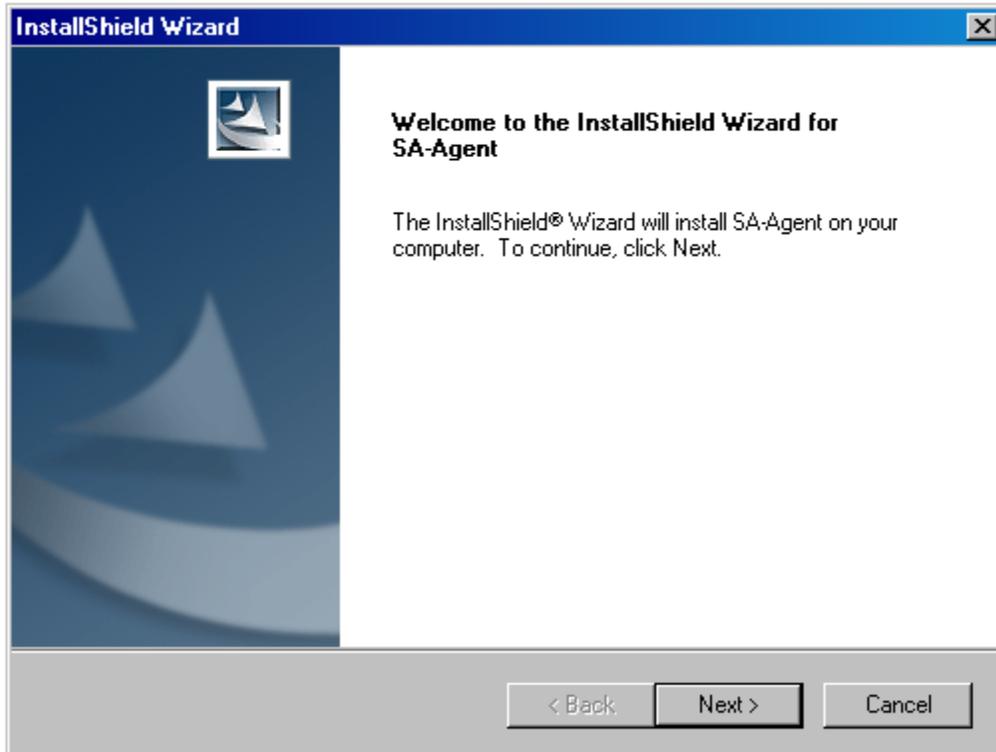
4. The License Agreement panel opens. Read the license agreement carefully. Click the **I accept the terms in the license agreement** button and click **Next**.
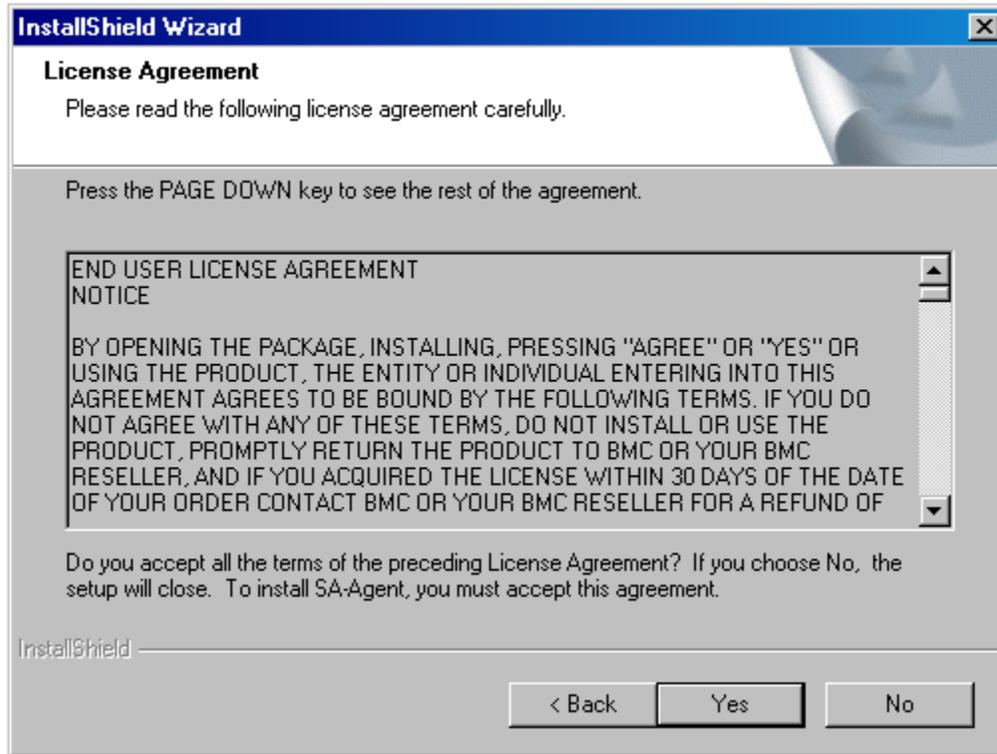
5. Select the installation path, or accept the default path. Click **Next**.
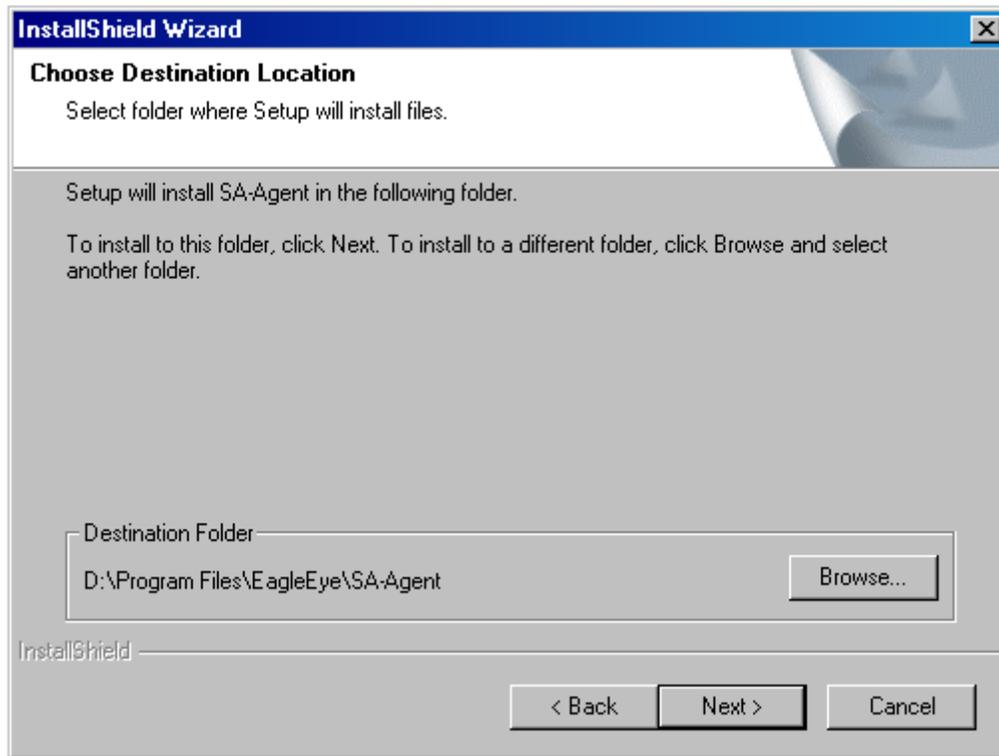
6. Select the **Encrypted** option for secure communication. Click **Next**.
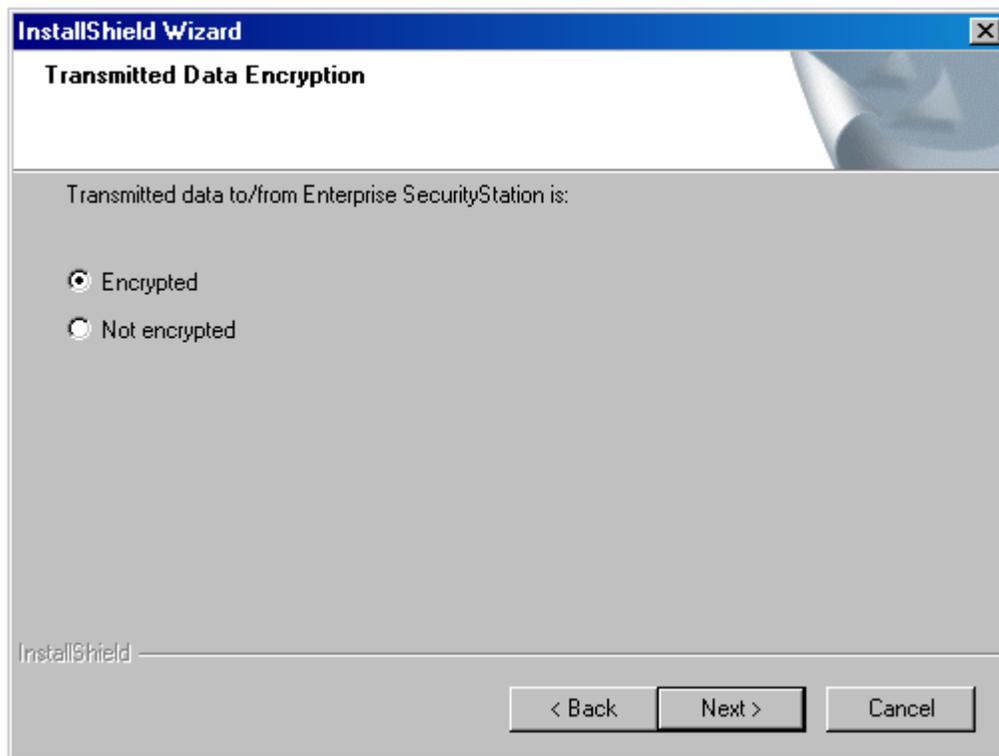
7. Enter **host name** or **IP address** of the system. Click **Next**.
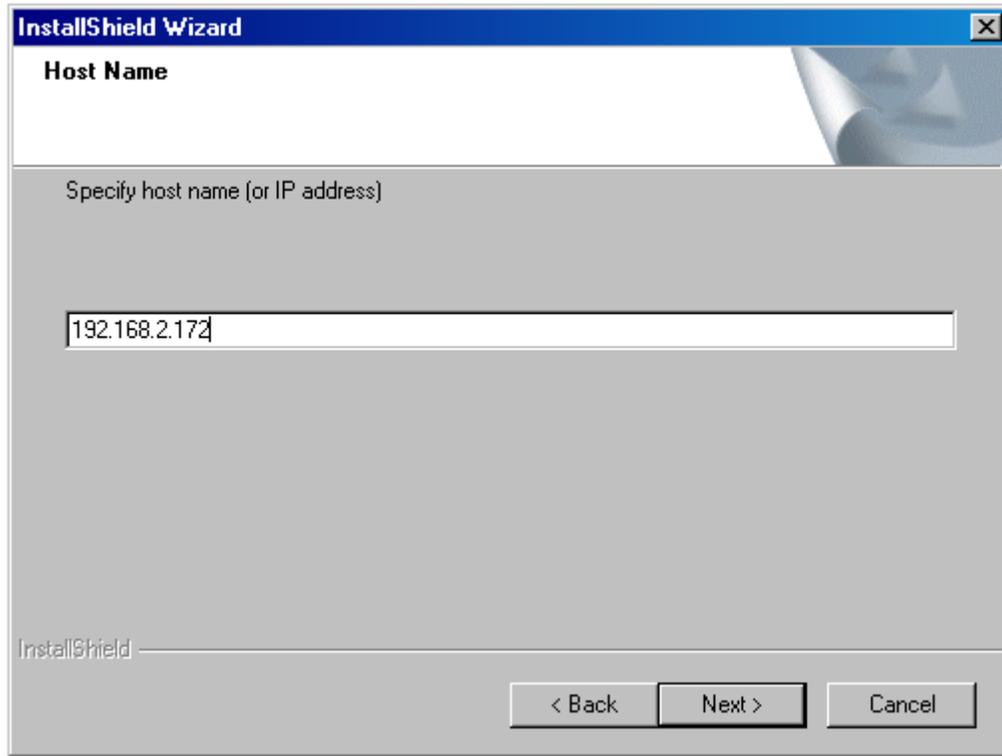
8. Enter the **TCP/IP Port Number** to be used for data transmission. Click **Next**.
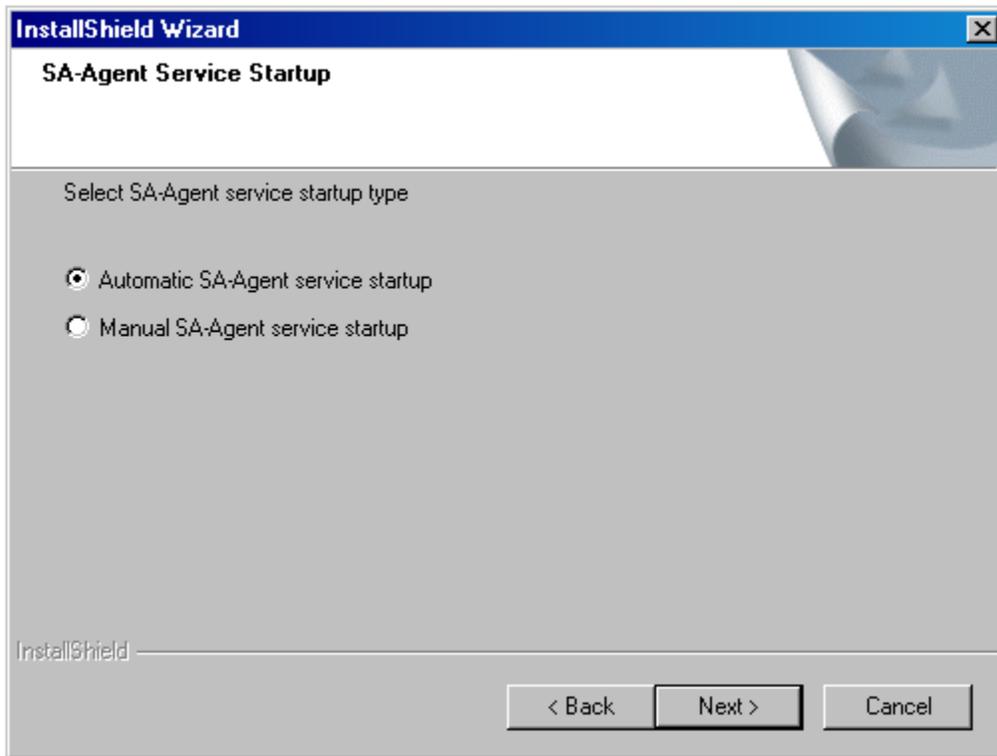
9. Click **Next**.

10. Click **Next** and wait for some time.
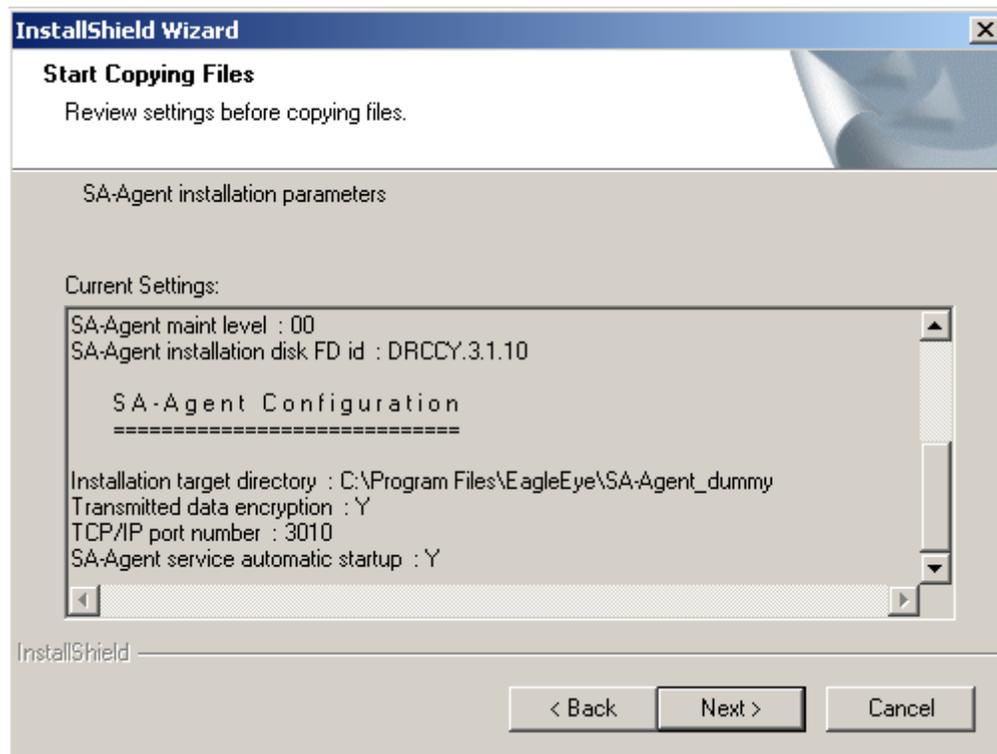
11. This is the final window of the installation. Click **Yes** and continue the configuration procedure. Please see the next section for instructions. Otherwise, click **No** to terminate the procedure.
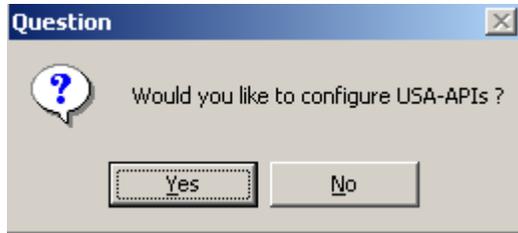
Configuring the CONTROL-SA Module

1. The Start menu on the Windows task bar contains a separate entry for each Instance ID, in the format SA-AgentInstanceId. For example, to configure the instance whose instance ID is New, select the following from the Start menu: **Programs** > **CONTROL-SA** >**SA-Agent** > **Add Managed System**.

2. Enter the Passlogix **Managed System name**.
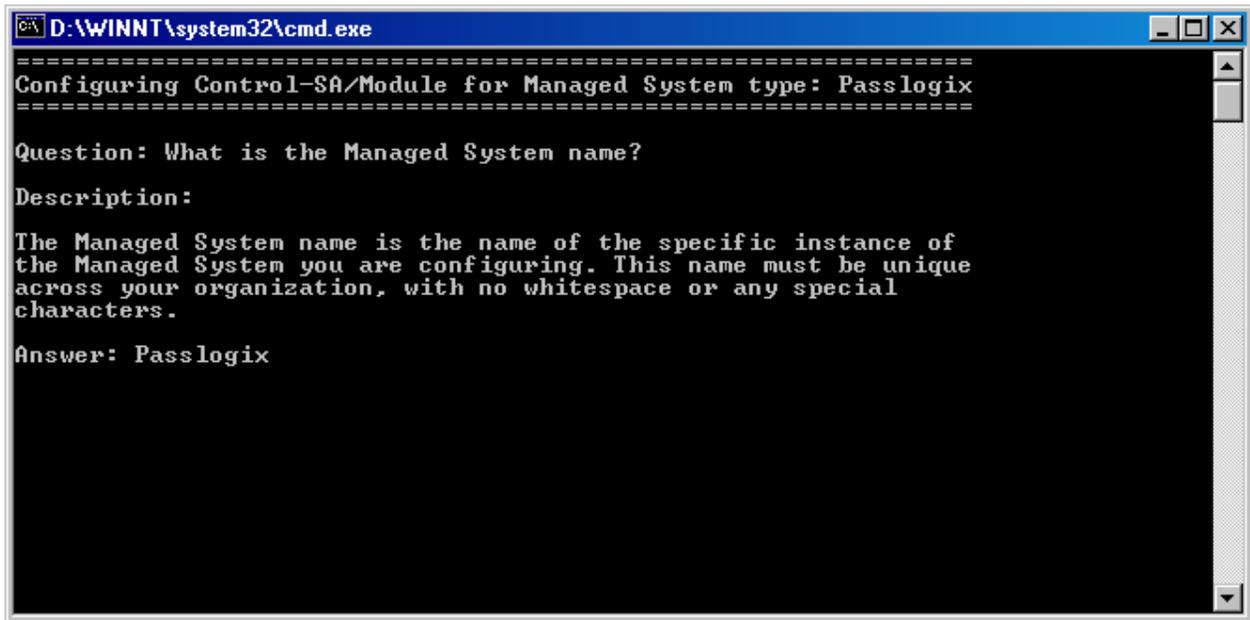
```
D:\WINNT\system32\cmd.exe                                          _ □ ×
============================================================
Configuring Control-SA/Module for Managed System type: Passlogix
============================================================

Question: What is the Managed System name?

Description:

The Managed System name is the name of the specific instance of
the Managed System you are configuring. This name must be unique
across your organization, with no whitespace or any special
characters.

Answer: Passlogix
```

3. Enter the **Managed System description**.

```
D:\WINNT\system32\cmd.exe                                    _ □ X

Question: What is the Managed System name?

Description:

The Managed System name is the name of the specific instance of
the Managed System you are configuring. This name must be unique
across your organization, with no whitespace or any special
characters.

Answer: Passlogix

====================

Question: What is the Managed System description?

Description:

The Managed System description is a free-text description of the
specific instance of the Managed System you are configuring.

Default: Control SA Agent for Passlogix Single Sign On
(press enter to keep the default value)

Answer: _
```

4. Enter the **default administrator account name** for the SA Agent. Any account
   that has access rights to the `v-go-pm-users.dat` file can be used here.

```
D:\WINNT\system32\cmd.exe                                    _ □ X

Question: What is the Managed System description?

Description:

The Managed System description is a free-text description of the
specific instance of the Managed System you are configuring.

Default: Control SA Agent for Passlogix Single Sign On
(press enter to keep the default value)

Answer:

====================

Question: Default administrator account name?

Description:

Default account name of administrator used for get actions.

Default: Administrator
(press enter to keep the default value)

Answer:
```

5.   Enter the **default administrator password**.

```
D:\WINNT\system32\cmd.exe                                          _ □ ×

Default: Control SA Agent for Passlogix Single Sign On
(press enter to keep the default value)

Answer:

====================

Question: Default administrator account name?

Description:

Default account name of administrator used for get actions.

Default: Administrator
(press enter to keep the default value)

Answer:

====================

Question: What is the default administrator password (Maximum
length is 32 characters)?

Password: ********
```

6.   Enter the **Offline Interceptor execution interval**. This interval's function is to
     check the `v-go-pm-users.dat` file for new users at the given interval.
     Note: This interval must be entered in the (HHMMSS) format. For instance, the a
     value of "010000" would equal 1 hour.

```
D:\WINNT\system32\cmd.exe                                          _ □ ×
Default: Administrator
(press enter to keep the default value)

Answer:

====================

Question: What is the default administrator password (Maximum
length is 32 characters)?

Password: ********

====================

Question: Offline Interceptor execution interval (HHMMSS)?

Description:

Time to wait between executions of the Offline Interceptor
(000000 for manual execution only).

Default: 010000
(press enter to keep the default value)

Answer:
```

7. Enter the **ESSO-PG Web Service URL**.

8. Enter the **Username to authenticate against the Web Service**.

9. Enter the **Password to authenticate against the Web Service**.
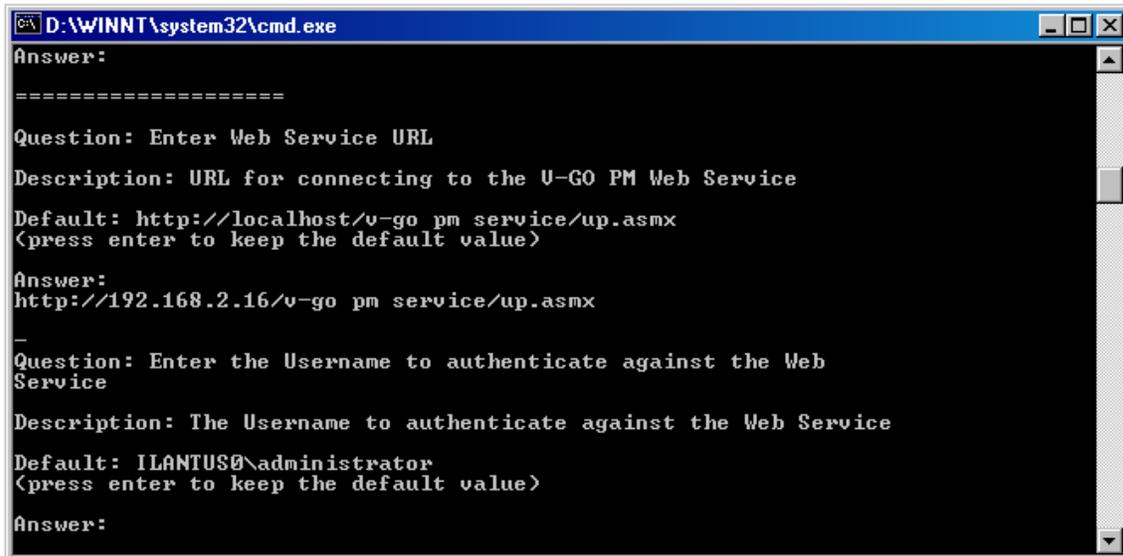
```
D:\WINNT\system32\cmd.exe                                          _ □ ×
Answer:
http://192.168.2.16/v-go pm service/up.asmx

_
Question: Enter the Username to authenticate against the Web
Service

Description: The Username to authenticate against the Web Service

Default: ILANTUS0\administrator
(press enter to keep the default value)

Answer:


_
Question: Enter the Password to authenticate against Web Service

Description: Password to authenticate against Web Service

Default: password
(press enter to keep the default value)

Answer:
```

10. Enter the **Identifier for this agent**.

```
D:\WINNT\system32\cmd.exe                                          _ □ ×
Answer:


_
Question: Enter the Password to authenticate against Web Service

Description: Password to authenticate against Web Service

Default: password
(press enter to keep the default value)

Answer:


_
Question: Please enter the Identifier for this agent

Description: Identifier for this agent. Default is machine name.

Default: kiran
(press enter to keep the default value)

Answer:
```

11. Enter **C** to Confirm the entries; otherwise, enter **R** for Retry or **A** to Abort the current values.
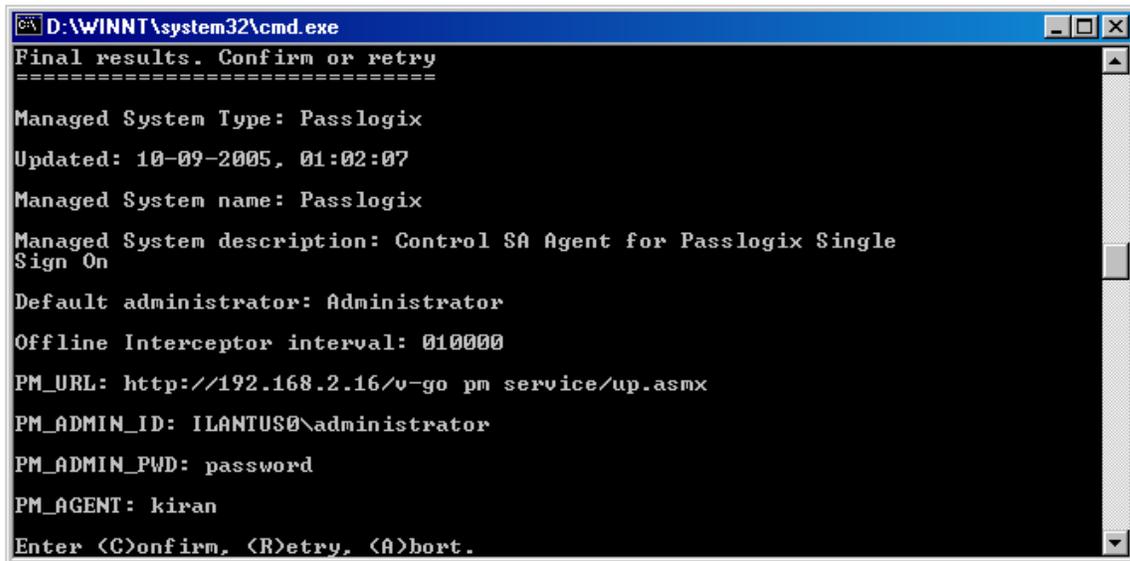
```
D:\WINNT\system32\cmd.exe                                    _ □ ×

Final results. Confirm or retry
===============================

Managed System Type: Passlogix

Updated: 10-09-2005, 01:02:07

Managed System name: Passlogix

Managed System description: Control SA Agent for Passlogix Single
Sign On

Default administrator: Administrator

Offline Interceptor interval: 010000

PM_URL: http://192.168.2.16/v-go pm service/up.asmx

PM_ADMIN_ID: ILANTUS0\administrator

PM_ADMIN_PWD: password

PM_AGENT: kiran

Enter (C)onfirm, (R)etry, (A)bort.
```

12. Enter **Y** to start the agent or **N** to restart later.
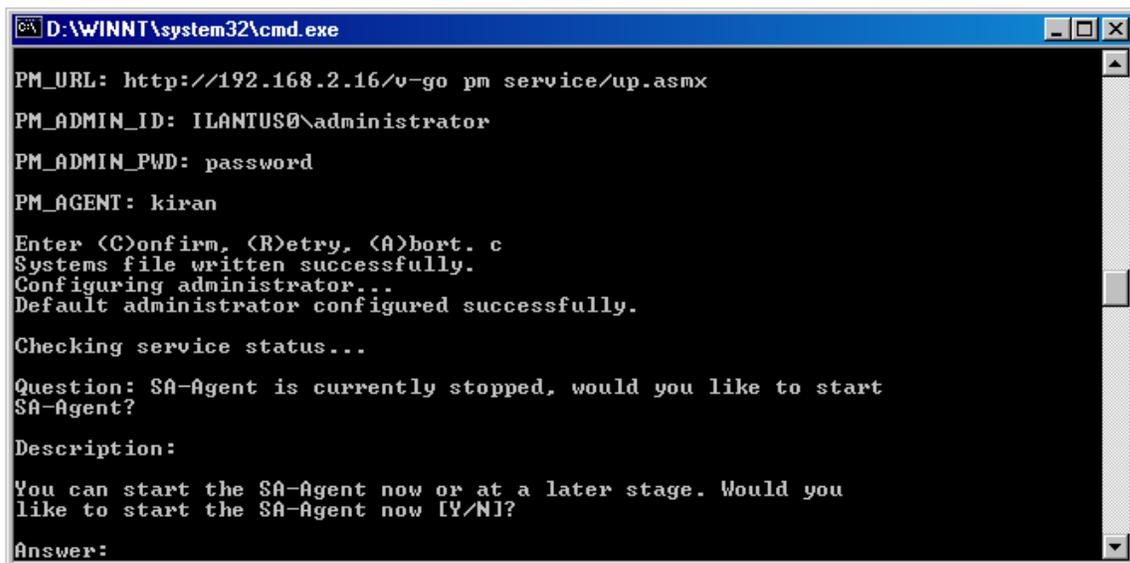
```
D:\WINNT\system32\cmd.exe                                    _ □ ×

PM_URL: http://192.168.2.16/v-go pm service/up.asmx

PM_ADMIN_ID: ILANTUS0\administrator

PM_ADMIN_PWD: password

PM_AGENT: kiran

Enter (C)onfirm, (R)etry, (A)bort. c
Systems file written successfully.
Configuring administrator...
Default administrator configured successfully.

Checking service status...

Question: SA-Agent is currently stopped, would you like to start
SA-Agent?

Description:

You can start the SA-Agent now or at a later stage. Would you
like to start the SA-Agent now [Y/N]?

Answer:
```

13. Click **Finish** to complete the installation.
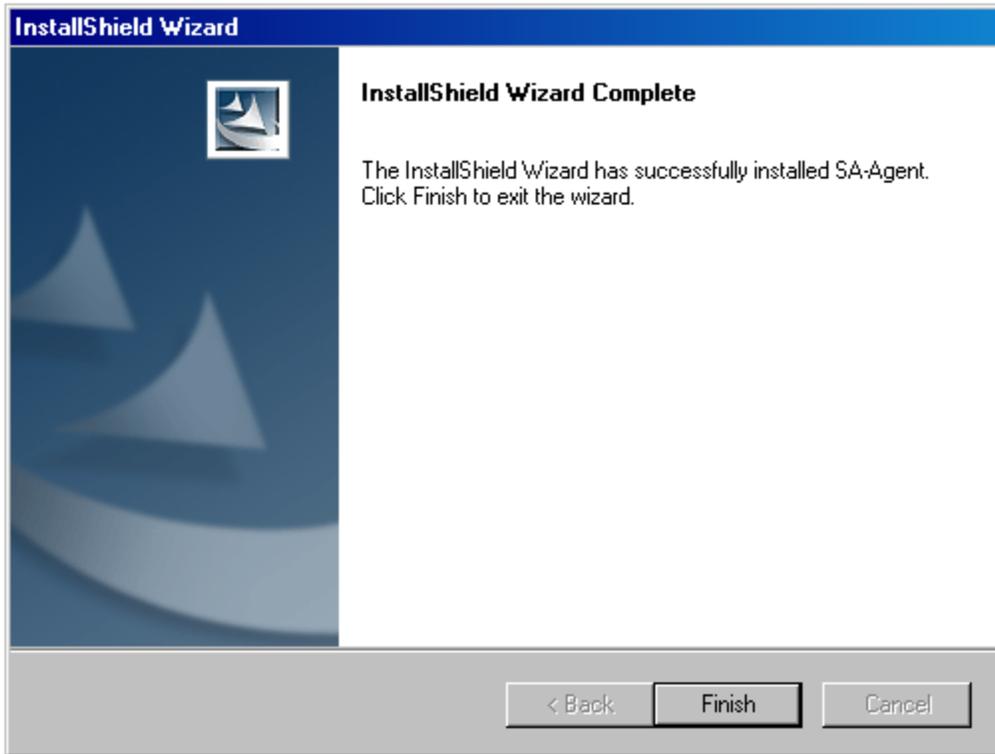
Patch to Support Additional Java Class PATH in the SA Agent

This patch is located in the Patch/PAXAG.3.6.02.002 directory.

PAXAG.3.6.02.002: Support Additional Java Class PATH

Summary
======
This patch provides support for additional class path for Java connectors.

This step is mandatory.
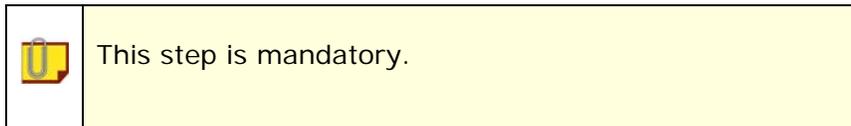
Affected Product
==========
CONTROL-SA/XModule Studio version 3.6.02
(for both Solaris and Microsoft Windows)

Files in this patch
===========
`XSA_LangJava.so` - the shared object which implements the fix
(Solaris version)
`XSA_LangJava.dll` - the dll which implements the fix (Windows
version)
`JavaLibPath.txt` - sample classpath file with a sample unix class path

Problem description
============
The Java engine module did not have a mechanism to receive
additional class path.

This problem has been resolved by updating the Java controller
shared/dll object (`XSA_LangJava.so/dll`) that is responsible for
loading the JVM.

The classpath is controlled by a new configuration file named
`JavaLibPath.txt`.

The path to the Java CLI (`pmcli.jar` and all supporting files) must be
added to the `JavaLibPath.txt` file. Each `.jar` file entry must be
separated by a semicolon on Windows and a colon on Unix. Add the
following to the `JavaLibPath.txt` file (each on separate lines for
clarity):

<path>`\PMCLI.jar;`
<path>`\activation.jar;`
<path>`\axis-1.2.1.jar;`
<path>`\bcprov-jdk13-128.jar;`
<path>`\commons-discovery-0.2.jar;`
<path>`\commons-logging-1.0.4.jar;`
<path>`\jaxrpc.jar;`
<path>`\log4j-1.2.9.jar;`
<path>`\mail.jar;`
<path>`\opensaml-1.0.1.jar;`
<path>`\saaj.jar;`
<path>`\wsdl4j-1.5.1.jar;`
<path>`\wss4j.jar;`
<path>`\xmlsec-1.2.1.jar;`

Replace **<path>** with the full path to the jar file and place each entry
on one unbroken line.

The Java CLI also requires that the following files be placed in the
`endorsed` directory of the Java CLI installation folder
(`%JAVA_HOME%\lib\endorsed`):

`dom.jar`
`jaxp-api.jar`
`sax.jar`
`xalan.jar`
`xercesImpl.jar`

To install the patch for Microsoft Windows
===========================

Note: This step is mandatory.

1. Back up XSA_LangJava.dll (located in the SA-Agent EXE directory).

2. The Patch can be found in the following directory:
   `<Passlogix Agent Directory>/PAXAG.3.6.02.002`

3. Unpack the file `PAXAG.3.6.02.002.zip` in a temporary directory. This file contains the following files:
   - `XSA_LangJava.so`
   - `XSA_LangJava.dll`
   - `JavaLibPath.txt`

4. Copy the new `XSA_LangJava.dll` to the `EXE` directory.

5. Do the following:

   a. Copy the file `JavaLibPath.txt` to the `<saAgentHome>\DATA` directory.
      For example, if the sample connector `TDB_JAVA` was installed under:

      `C:\Program Files\EagleEye\SA-Agent\`

      the file location should be:

      `C:\Program Files\EagleEye\SA-Agent\DATA\JavaLibPath.txt`

   b. Open JavaLibPath.txt in a text editor; replace the sample classpath with the appropriate classpath. Reminder - the path separator in Windows is ';'

      If the JavaLibPath.txt file does not exist or is empty - no additional "classpath" will be used.

   c. Save the file.

Copy the flat file containing ESSO-PG Users

> It is mandatory that the users are entered in this file. This is the file that the SA Agent checks at the given interval defined in step 6 on Page 17.

The filename of the ASCII flat file should be:

> **v-go-pm-users.dat**

It should be placed in the following folder:

> **<SA-Agent-Installation-Directory>\WORK\Passlogix**

where SA-Agent-Installation-Directory - is the SA Agent Installation Directory.

For example: The contents of the ASCII flat file should be:

> **User1**
> **User2**
> **User3**
> **User4**
> **.**
> **.**
> **.**
> **User<n>**

Where
User1, User2,…,User<n> - are the SSO User IDs.

> Every line should contain only one user. Do not leave any blank lines between users.

Uninstalling the USA—API

SA-Agent can be uninstalled using the **Add/Remove Programs** facility in the Windows Control Panel.

If more than one instance of SA-Agent exists, you have the option of uninstalling a selected instance without affecting other instances:

1. From the Windows Start menu, select **Settings** > **Control Panel** > **Add/Remove Programs**.

2. In the list of installed programs, select **SA-Agent**; then click **Add/Remove**.

3. If more than one instance of SA-Agent exists, you can choose between removing one instance or all instances of SA-Agent.

> Passlogix strongly recommends that you close all active Windows applications before starting the uninstall procedure.
>
> If you chose to remove one instance of SA-Agent, in the next window, select the instance ID to be removed.
>
> Upon completion, the message, *The deletion completed successfully*, is displayed.

Oracle ESSO-PG USA-API Interaction

The USA–API is designed to interact with ESSO-PG and update or retrieve information from it. These activities are performed for the following functions:

- User definitions

- User Group definitions

- User-to-User Group Connection definitions

Agent Function List

Names and descriptions of agent functions are listed below according to entity type or function.

RSS User Functions	Description
AccountGet	Retrieves RSS User data
AccountDelete	Deletes RSS User

User Group Functions	Description
GroupGet	Retrieves user group details

User-to-User Group Connection Functions	Description
ConnectionGet	Retrieves user-to-user group connection details
ConnectionAdd	Adds a new connection
ConnectionUpdate	Updates an existing connection
ConnectionDelete	Deletes a connection.

Appendix

Resources Utilization

The USA-API utilizes the following system resources during its execution:

- Memory

- CPU

The USA-API modules free the resources during termination.

Memory Usage

The memory usage depends on the amount of data being downloaded during the execution of GET functions. During the download, the maximum memory usage ranges from 15 to 20 MB. (This estimate is for 20 users, 10 groups, and 15 connections.)

During the execution of SET functions, the maximum memory usage ranges from 3 to 5 MB.

Data Storage

The USA–API for Passlogix ESSO-PG uses the standard Agent messaging facility as well as the CONTROL-SA logging facility. These logs should be cleaned up at regular intervals. Automatic log maintenance facility of the agent can be used. Refer to Section 7, Page 7-32, in the *CONTROL-SA Agent for Windows 2000 – Administrator Guide* for details on how to implement automatic log maintenance.

Protocol Security

The client communicates to the server using the standard TCP/IP protocol with SSL encryption.

Messages

The USA-API is designed to write messages during execution of the functions into the log files. These log files can be found in the SA Agent\Log Directory.

Keywords

RSS User Keywords

RSS User Functions
gu Get users
du Delete user

None

RSS User Group Keywords

RSS User Group Functions
gug Get user groups

None

RSS User-to-User Group Connection Keywords

RSS User Group Functions
gug   Get user-to-user group connections
auug   Add user-to-user group connection
uuug   Update to user group connection
duug   Delete to user group connection

ESSO-PG Parameters

Internal Field Name	GUI Field label	T	Len	guug	auug	uuug	duug
sso_description	SSO Description	C	50	x	x	x	
sso_app_userid	SSO Application Userid	C	32	x	x	x	x
sso_password	SSO Password	C	32	x	m	x	x
sso_other1	SSO Other1	C	32	x	x	x	x
sso_other2	SSO Other2	C	32	x	x	x	x

Legend

m   – Mandatory keyword
x   – Optional keyword
T   – Data Type of the input accepted in the field (C-Char; F-Flag; N-Integer)
Len   – Length of the field

Glossary

API	Application Programming Interface. The interface that translates the ESS commands to the native commands of application to be managed using CONTROL-SA.
CONTROL-SA	CONTROL-SA is an integrated client-server solution, including ENTERPRISE SECURITY STATION and SA-Agent running on multiple platforms throughout your organization
Entity	An entity defines a component used for security administration by ENTERPRISE SECURITY STATION. For example, enterprise users or user groups.
GUI	Graphical User Interface. The ENTERPRISE SECURITY STATION GUI provides operator access to the facilities and windows of ENTERPRISE SECURITY STATION through a simple graphical tool.
RSS	The resident security system (RSS) is a security product or module. The RSS can be the native security of an operating system (such as, Solaris, HP-UX, or Novell NetWare), an add-on security product (such as, RACF or SeOS), or any other product that requires user registration (such as, Sybase or Oracle).
RSS Administrator	Entity that describes an administrator in an RSS. The USA-API actions on the native system are executed in the RSS using the login ID of the RSS administrator.
Default Administrator	Entity that describes the administrator for performing Read Operations on the RSS.
SA-Agent	Security administration agent running on platforms administered by ENTERPRISE SECURITY STATION.
Platform	Platform on which SA-Agent runs. This platform contains the USA–APIs for each type of RSS managed by ENTERPRISE SECURITY STATION via the platform.
SA-Agent Queue	File on the SA-Agent platform in which security events (such as, definition of new user) are recorded. These events are transmitted to ENTERPRISE SECURITY STATION. If communication with the ESS gateway is temporarily interrupted, the events are accumulated in the queue until communication is restored.