Paper SAS5680-2016

Advanced Topics in SAS® Environment Manager

Zhiyong Li and Gilles Chrzaszcz, SAS Institute Inc.

ABSTRACT

Since it was first released three years ago, SAS® Environment Manager has been used widely in many customers' production environment. Customers are now familiar with the basic functions of the product. They are asking for more information about advanced topics such as how to manage users, roles, and permissions; how to secure the product; and how to interact with their existing system management tools in their enterprise environment. This paper addresses those advanced but practical issues from a real customer's perspective. The paper first briefly lists what's new in the most current release of SAS Environment Manager. It then discusses the new user management design introduced in the third maintenance release of SAS 9.4. We explain how that design addresses customers' concerns and the best practices for using that design and for setting up user roles and permissions. We also discuss the new process and best practices for configuring SSL for SAS Environment Manager. More and more customers have expressed an interest in integrating SAS Environment Manager with their own system management tools. Our discussion ends with explaining how customers can do that through the SNMP interface built into SAS Environment Manager.

INTRODUCTION

SAS Environment Manager was first introduced as a new product with the release of SAS 9.4. It was widely adopted immediately, and many customers used it for their administration, monitoring and troubleshooting needs. Over the last three years, the product functions have been improved dramatically, and customers have become more interested in exploring these improved functions as well as other advanced features. This paper will first introduce the key new features introduced in the third maintenance release of SAS 9.4 and then discuss the following three advanced topics in SAS Environment Manager.

1. User management has been improved in each of the maintenance releases. With the release of the third maintenance release of SAS 9.4, it is now functioning the way we want it to be. We will discuss the new user management function introduced in SAS 9.4M3. We will explain how that design addresses customers' concerns. We will also go over the best practices for using the design and for setting up user roles and permissions.
2. Many people want to configure SAS Environment Manager to use SSL, but this configuration has been problematic. The problems are due to the advanced nature of SSL configuration itself, as well as to the distributed nature of SAS Environment Manager architecture and how it interacts with other SAS middle tier components. We will discuss the new process and best practices for configuring SSL for SAS Environment Manager introduced in the third maintenance release of SAS 9.4.
3. SNMP support has been in SAS Environment Manager since the first release. However, we have left it to customers to figure out how this support can be used in their environment. As more customers become interested in this function, a real world example will help customers to implement their integration of SAS Environment Manager with their customer environment.

NEW FEATURES IN 9.4M3

In addition to numerous defect fixes, SAS Environment Manager 2.5, which runs on the third maintenance release for SAS 9.4, has the following new features and enhancements:

- Support has been added in SAS Environment Manager Administration for managing metadata definitions for SAS users, servers, and libraries. User definitions can be viewed, created, and edited. Server and library definitions can be viewed, and SAS LASR libraries and servers and Base SAS libraries can be created and edited.

- Customers have a consistent user interface and to view users defined in the SAS Metadata Server as well as users defined in SAS Environment Manager.
- The method for synchronizing users between SAS Environment Manager and the SAS Metadata Server has changed. Instead of synchronizing metadata accounts, the process synchronizes metadata users.
- The reports in the Report Center (part of the service architecture) have been changed from stored process report objects to stored process objects, which makes the reports more dynamic. The reports are now re-generated at every request, rather than being cached after the first time they are generated. Each stored process is generated using prompts that enable you to alter the contents and appearance of the report. The SAS Environment Management Data Mart now supports a federated data mart. A federated data mart enables you to collect metric data in data marts for several SAS deployments, copy that data to a single collector deployment, and view the collected metric data in one place.
- Log collection and discovery has been improved. Rather than relying on log locations that are stored in metadata, the ETL processes look through the directory structure of a SAS deployment to find log files.
- Support has been added for collecting metric data from a SAS grid. Metric data is collected and reported upon for the grid and for individual grid nodes.
- The new SAS Backup Manager is available on the Administration tab.
- Many security-related updates have been made so that SAS Environment Manager can pass the AppScan security scanning.

USER MANAGEMENT

The most important change in SAS Environment Manager user management for the third maintenance release of 9.4 is that users, rather than accounts, defined in the SAS Metadata Server are synchronized as SAS Environment Manager users. This design addresses several customer concerns including:

- Confusion resulting from users in the SAS Metadata Server and SAS Environment Manager not being consistent. SAS Metadata Server users do not exist in SAS Environment Manager, although their accounts exist.
- One user in the SAS Metadata Server that has multiple accounts would result in multiple users being defined in SAS Environment Manager.
- Users might encounter case sensitivity issues when they log on to SAS Environment Manager. Case sensitivity is inconsistent between the SAS Metadata Server and SAS Environment Manager.
    - User name is case sensitive in the SAS Metadata Server. The case sensitivity for authentication is based on the authentication providers (for example, the case sensitivity is different between Windows and UNIX).
    - User name in SAS Environment Manager is case insensitive. A case insensitive user is also used for authenticating the user.

With this improved design, we recommend the following process to create a user and use it in a SAS Environment Manager.

1. Create a user in SAS Metadata Server. You can create the user by using the SAS Environment Manager Administration tab or SAS Management Console. After you create the user, you must associate the user with one of these three SAS Metadata Server groups: SAS_EV_Super_User, SAS_EV_Guest, or SAS_EV_AppServer_Tier.

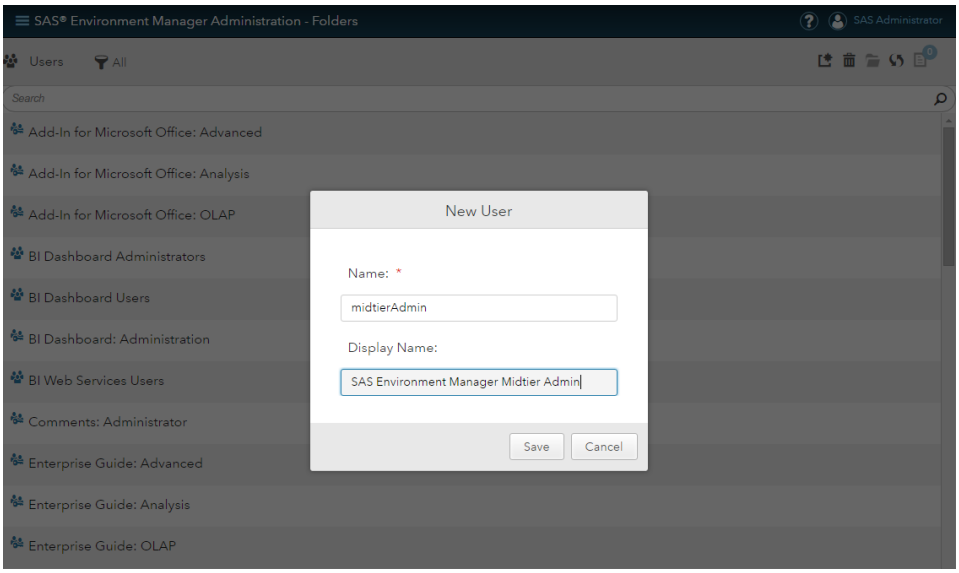
a. If you know you will use this user as either a SuperUser, a guest or a user to use SAS Application Server tier resources, you can simply select the corresponding group to be associated for the user.
b. If you plan to assign different roles or permissions to the user other than the three pre-defined, assign the user to the SAS Metadata Server group that is closest to the roles or permissions that the user needs.

2. Synchronize the user to SAS Environment Manager. After the user is defined in the SAS Metadata Server, you can either use the “Synchronize” function to synchronize the user into SAS Environment Manager or you can user that user’s credential to log on to SAS Environment Manager.
3. Assign the user to the SAS Environment Manager role. The user synchronized from the SAS Metadata Server has the role that is pre-defined between the Group in the metadata server and the role in SAS Environment Manager. You can change the role after the user has been synchronized.
4. Log on as the new user.

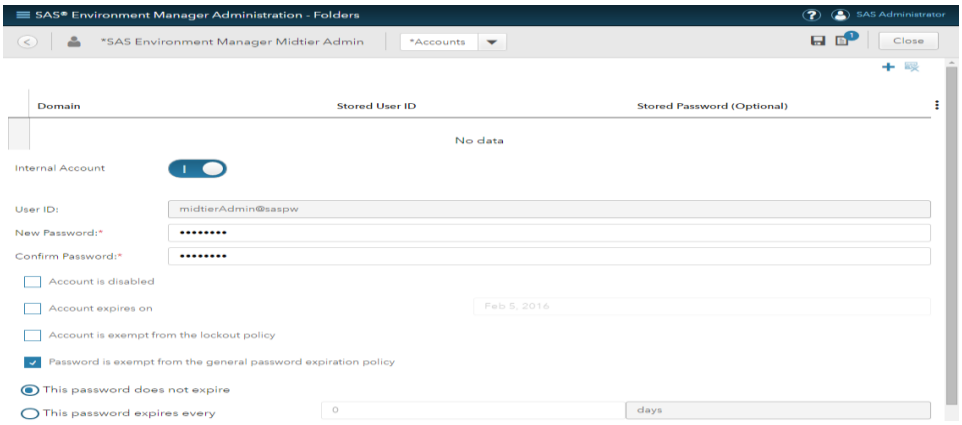
The following steps are an example of the user creation process. We want to create a user called midtierAdmin to manage the SAS middle tier components. We will create a role that is responsible for managing the middle tier and the middle tier applications, and assign the midtierAdmin user to that role.

STEP 1: CREATE A USER USING ADMINISTRATION

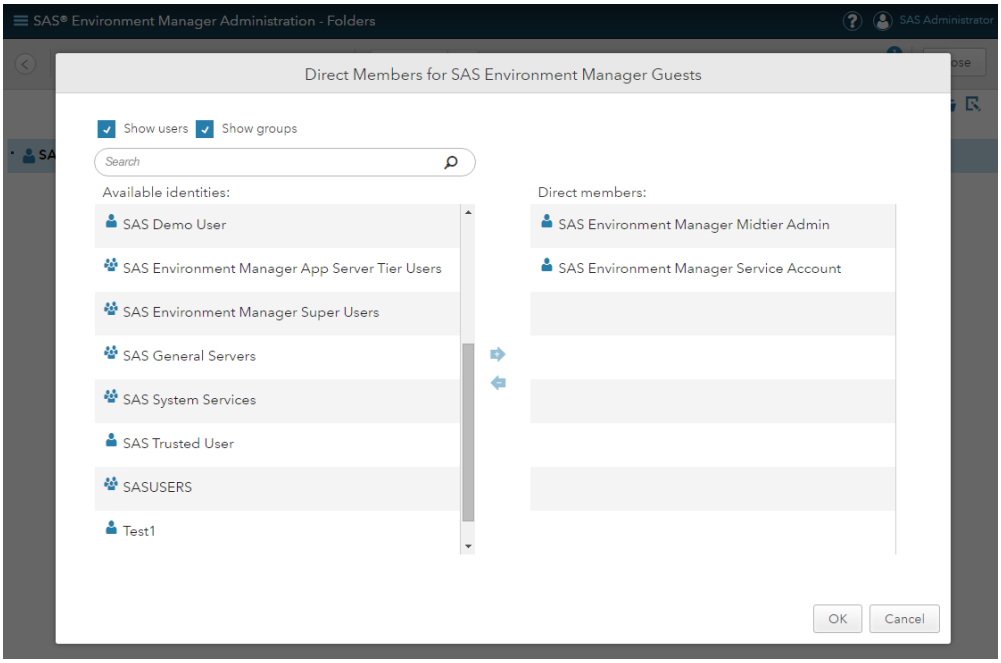
In SAS Environment Manager, select **Administration ➤ Users**, then **New User** from the drop-down list.



After you specify and save the information for the midtierAdmin user, select **Accounts** from the **Basic Properties** drop-down list. Create an internal account, provide a password, then select **Save**.

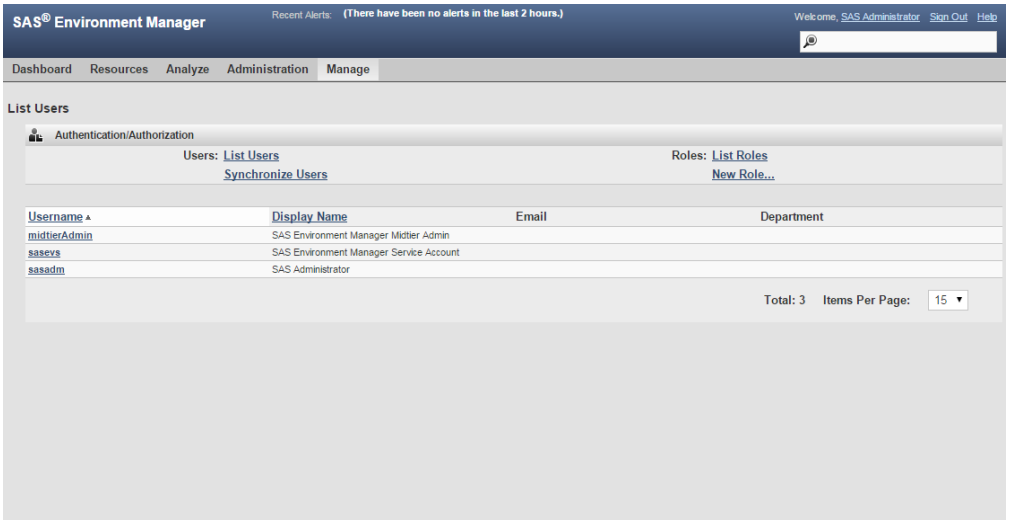


Return to the **Administration ➤ Users** list and select **SAS Environment Manager Guests**. Select **Basic Properties ➤ Members**. Edit **Members** to add the midtierAdmin user to the SAS Environment Manager Guests group.



STEP 2: SYNCHRONIZE USERS TO SAS ENVIRONMENT MANAGER

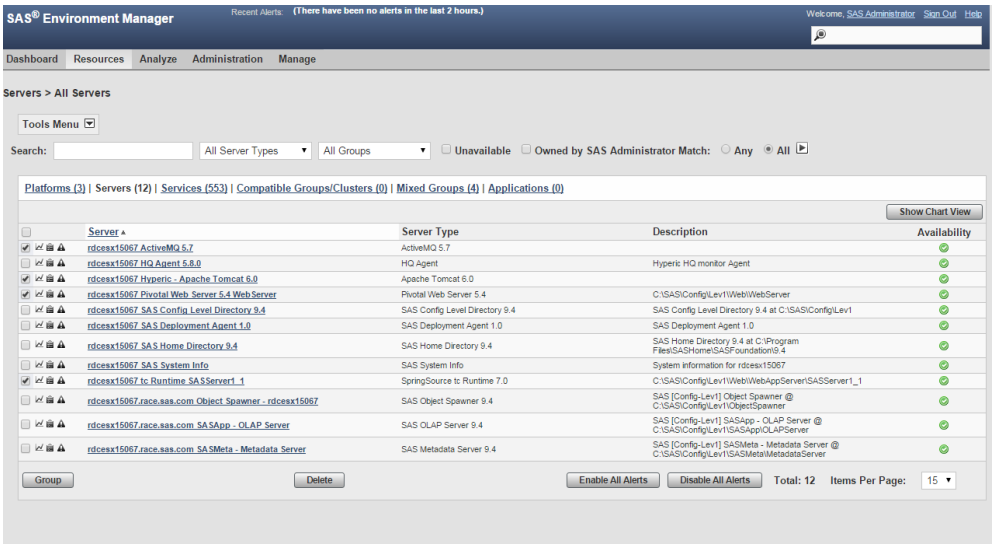
Select the SAS Environment Manager **Manage** tab, then **Synchronize Users**. When you select **List Users**, the midtierAdmin user is listed as shown below.



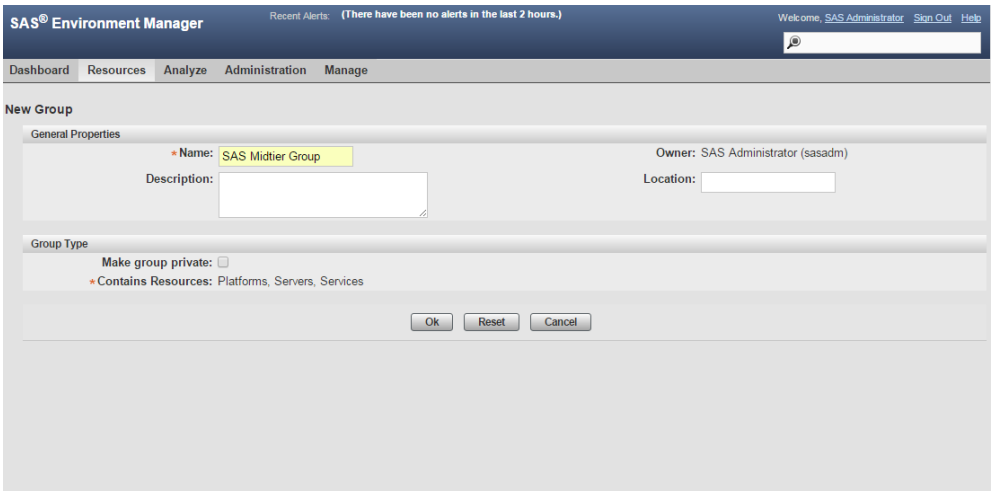
Select **midtierAdmin** from the list. You will notice that it has a Guest Role listed under **Roles Assigned To**.

STEP 3: CREATE A NEW ROLE

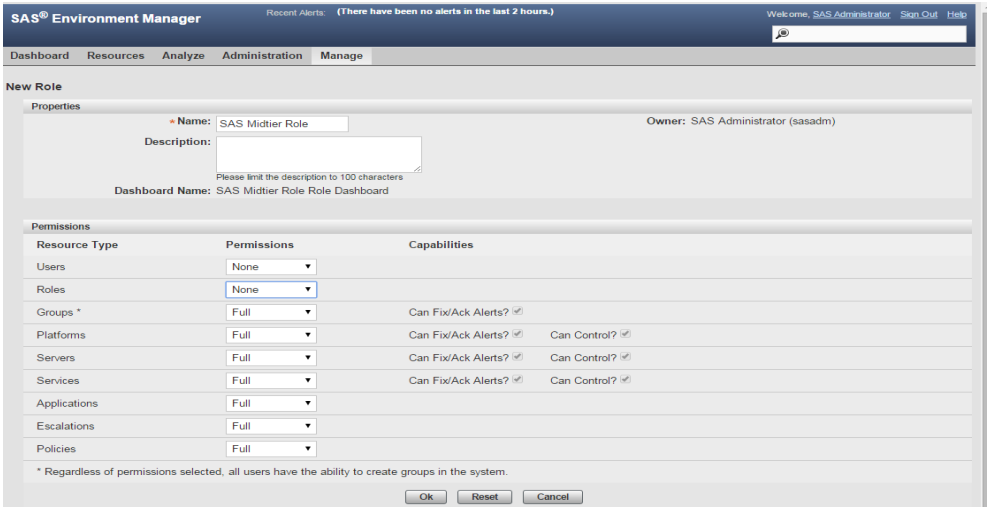
Before creating the role, create a group that will be used in the role. Select **Browse ➤ Servers**, then all middle tier servers that you want to be included in the group. Select **Create**.



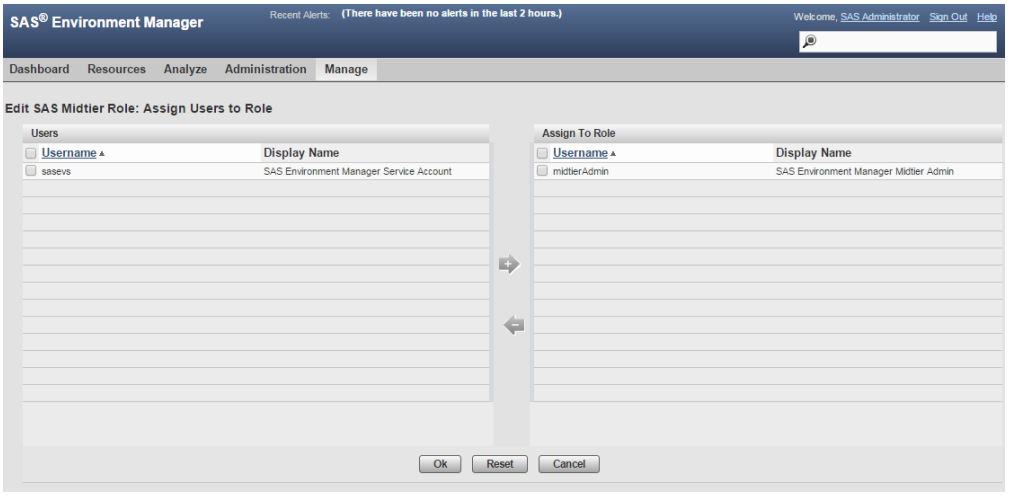
In the following screen, specify **SAS Midtier Group** as the name of the group.



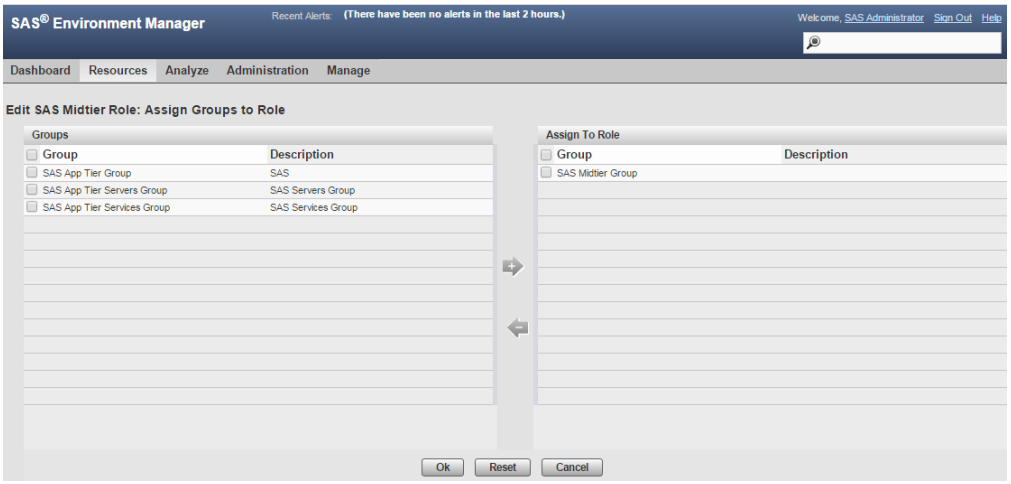
Select **Manage ➤ New Roles** and create a new role called SAS Midtier Role.



For the newly created role, select **Add to List** under **Assigned Users**, then add **midtierAdmin** to the role:

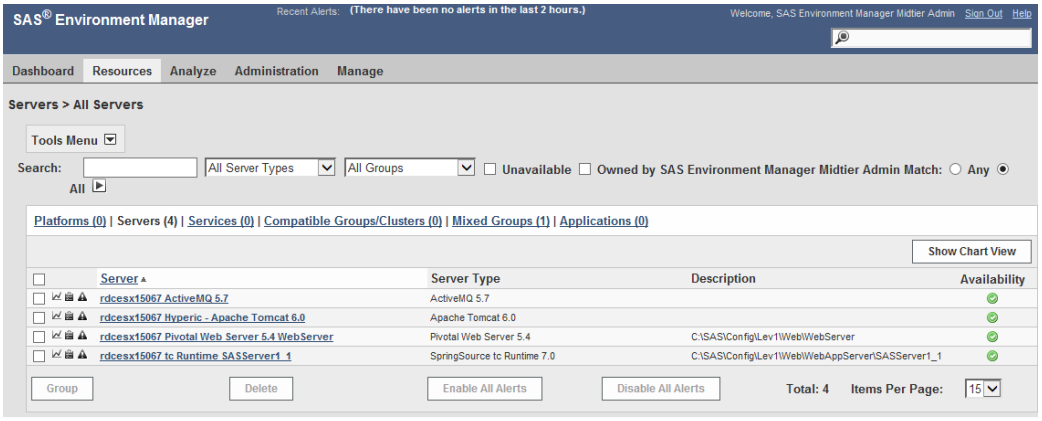


Select **Add to List** under **Assigned Groups** and add **SAS Midtier Group** into the **Group**.



STEP 3: LOG ON AS THE NEW USER

Log on to SAS Environment Manager as midtierAdmin@saspw. When you select **Resources**, you will see that you can view only middle tier servers as the Midtier Admin.



The SAS middle tier can also include services that are associated with the middle tier servers. If you want to allow the Midtier Admin to also be able to view services, you must edit the SAS Midtier Group and include the services you want the Midtier Admin to monitor or view.

SSL CONFIGURATION FOR SAS ENVIRONMENT MANAGER

CHANGES TO SSL SECURITY IN SAS 9.4M3

A typical process to deploy SAS 9.4 software consists of completing the following tasks:

1. Review installation documentation.
2. Create operating system users and groups, and designate ports.
3. Create a SAS Software Depot.
4. Install required third-party software.
5. (Optional) Configure SSL (or set up certificates).
6. Install and configure SAS software.

If you have a requirement to use SSL to secure communication between SAS web applications, then step five in the previous procedure is required. However, configuring SSL is not a trivial task. SAS has strived to make that process easier, and has been making improvement over each of SAS major and maintenance releases.

The third maintenance release of SAS 9.4 has made several improvements to the SSL security including:

- SAS provides a default truststore (the jssecacerts file) that takes precedence over the previous truststore (the cacerts file) in the SAS Private JRE.
- The trusted certificate authority (CA) bundle is a copy of the Mozilla bundle, which is the list of CA certificates that are distributed with Mozilla software products. (For more information, see"CA:Included CAs", available at https://wiki.mozilla.org/CA:IncludedCAs.)
- Certificate bundle management has been added to SAS Deployment Manager. Using SAS Deployment Manager, you can add and remove certificates to and from the trusted CA bundle. (For more information, see "Add Your Certificates to the Trusted CA Bundle" in *SAS 9.4 Intelligence Platform Installation and Configuration Guide, Second Edition*.)
    a. Prior to the third maintenance release for SAS 9.4, you must add your CA certificates to the SAS Private JRE using the keytool -importcert command. For more information, see "Add Your Certificates to the SAS Private JRE" in *SAS 9.4 Intelligence Platform Installation and Configuration Guide, Second Edition*.

The above improvements are applicable to all SAS components that can use SSL. However, in this paper, we will focus on how SAS Environment Manager takes advantage of the above changes.

Keep in mind, the newer generation of SSL security is also referred to as Transport Layer Security (TLS) or HTTPS security. TLS and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that are designed to provide communication security over the Internet. TLS and SSL are protocols that provide network data privacy, data integrity, and authentication. Note: All discussion of TLS is applicable to the predecessor protocol, SSL. In our discussion, we treat them as the same.

BEST PRACTICE OF SSL CONFIGURATION FOR SAS ENVIRONMENT MANAGER

SAS Environment Manager has two major components: the server and the agents. Each can be configured to use SSL. Therefore, it is possible to have four different combinations or scenarios:

1. Server: non-SSL; agents: non-SSL
2. Server: non-SSL; agents: SSL
3. Server: SSL; agents: non-SSL
4. Server: SSL; agents: SSL

In each scenario, a customer can choose to use self-signed, site-signed, or third party CA-signed certificates. It is also possible that a combination of the above certificates is used in one scenario. Some additional notes related with the certificate configuration are worthy of mention:

- Self-signed certificates can be automatically generated by the SAS Deployment Wizard, or they can be provided by customers.
- Provided certificates can be site-signed or CA signed.
- Customers can use the combination of automatically generated certificates and provided certificates

The current SAS Deployment Wizard allows you to configure all of above scenarios and choose different types of certificates for either the SAS Environment Manager server or agents. However, in practice, certain scenarios (such as Scenario 3; server – SSL, agents – non-SSL) might not make sense. When choosing which scenario to use in your deployment, you should also consider whether your web server is configured to use SSL. Our recommendations are as follows:

- If SAS Web Application Server is configured to use SSL, then use Scenario 4 for SAS Environment Manager.
- If SAS Web Application Server is not configured to use SSL, then Scenario 1 is preferred. However, you might consider using Scenario 2, because it can be configured without incurring extra costs if self-signed certificates are used.

For certificates, the best practice is as follows:

- For the agents, always use self-signed certificates that are generated by SAS Deployment Wizard. Because the agents' and server's connections are typically behind your firewall and do not involve users, there is less of a reason to implement third-party-signed certificates.
- For the server, use the same type of certificates that you are using for your other middle tier components that you have configured to use SSL.

Even if you are planning to provide your own certificates, we recommend that you accept the default and let SAS Deployment Wizard install auto-generated self-signed certificates for you, instead of providing your own certificates to SAS Environment Manager during installation. After SAS Deployment Wizard finishes, you can go back and replace the default SAS Environment Manager auto-generated JKS keystore with certificates that you provide. Choosing "Generate a default JKS format keystore" from the SAS Environment Manager configuration window saves you several manual configuration steps.

EXAMPLE BEST PRACTICE

In this example, we will show you how to use SAS Deployment Wizard to configure Scenario 4 and implement the recommendations for certificates. In summary, the configuration for this example is as follows:

- Server: SSL; agents: SSL
- Server: CA-certificates, agents: self-signed certificates.

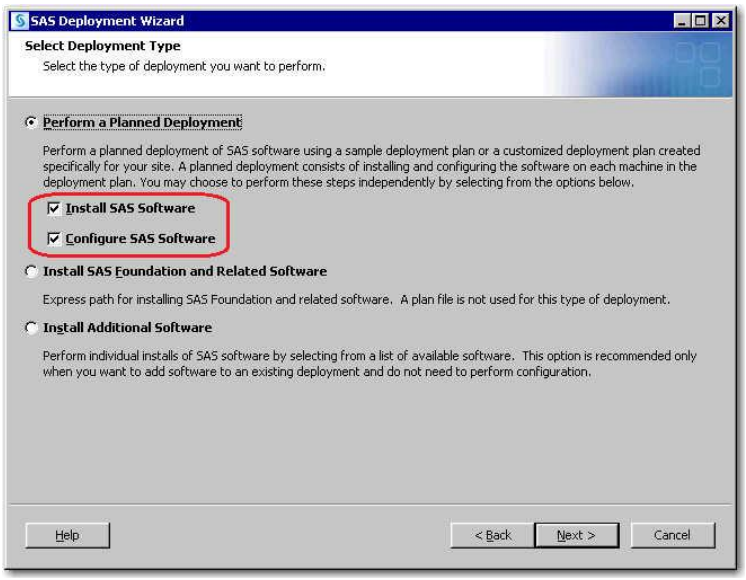
There are four steps in the configuration process:

1. SAS Environment Manager pre-configuration
2. SAS Environment Manager server configuration
3. SAS Environment Manager agent configuration
4. SAS Environment Manager post-configuration

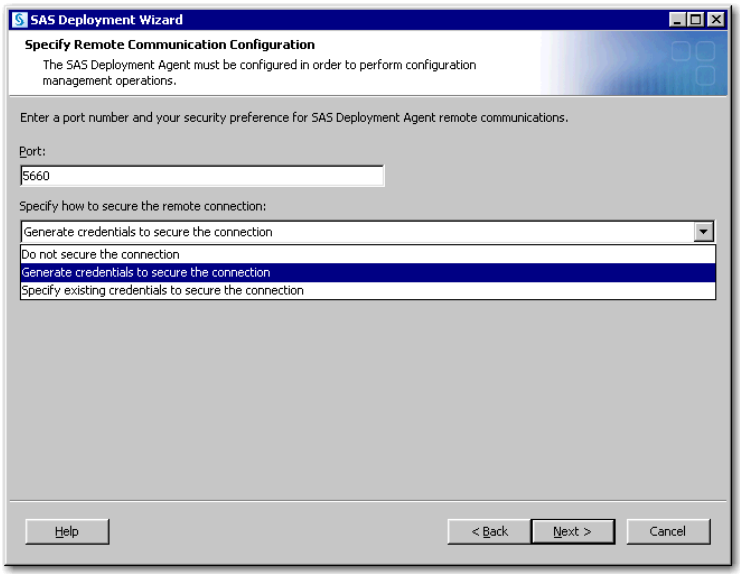
SAS Environment Manager Pre-Configuration

Before you start working with the SAS Environment Manager section of SAS Deployment Wizard, you must specify several pieces of information that might impact the SAS Environment Manager SSL configuration.

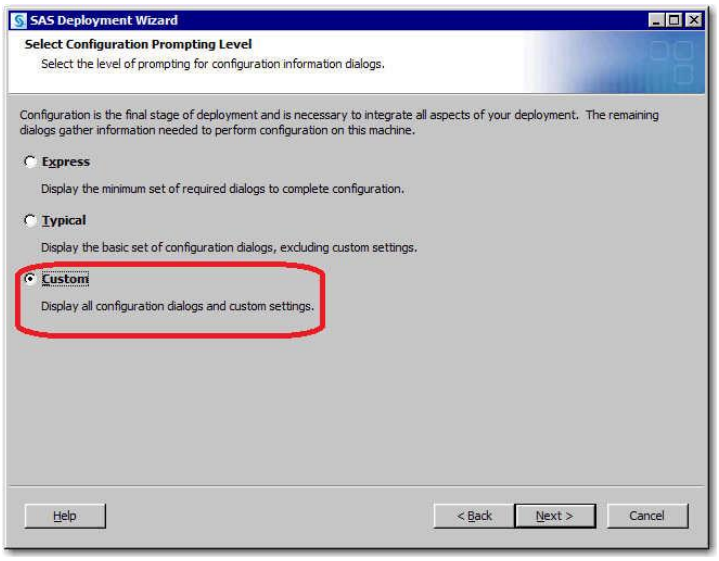
1. Run SAS Deployment Wizard. Make sure that both **Install SAS Software** and **Configure SAS Software** are selected.



2. When you are prompted for the SAS Deployment Agent remote communication configuration, select **Generate credentials to secure the connection**.

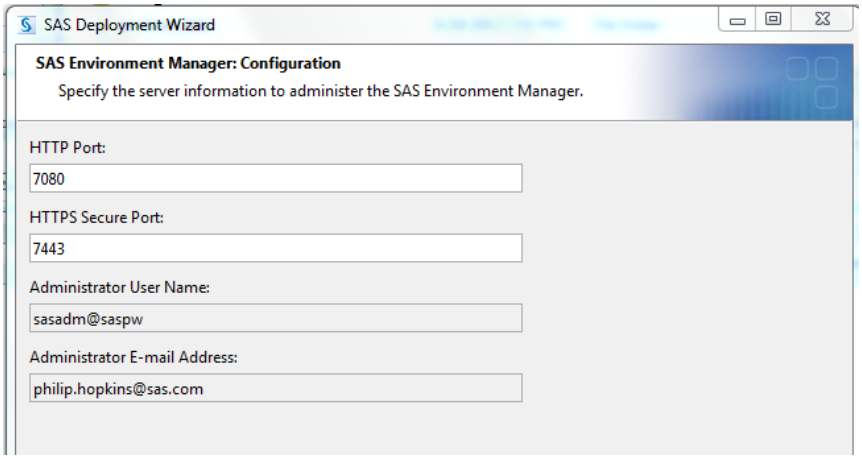


3. When you are prompted for the configuration prompting level, select **Custom**.

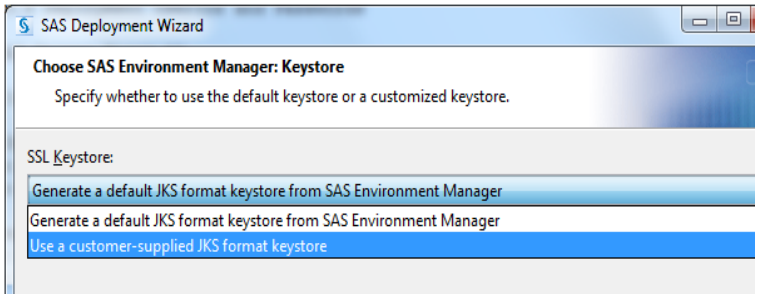


SAS Environment Manager Server Configuration

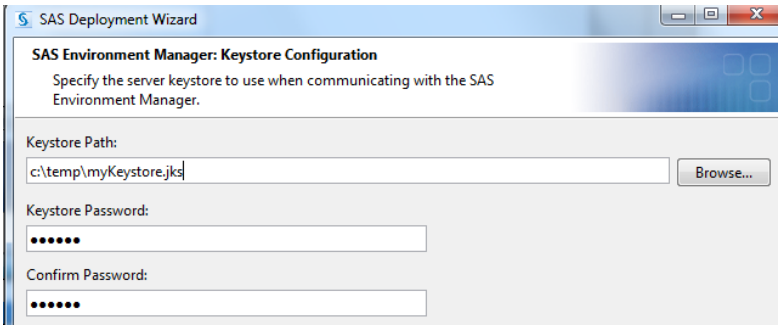
1. You start at the following window. You can usually use the default values for the ports.



2. Select **Use a customer-supplied JKS format keystore**.

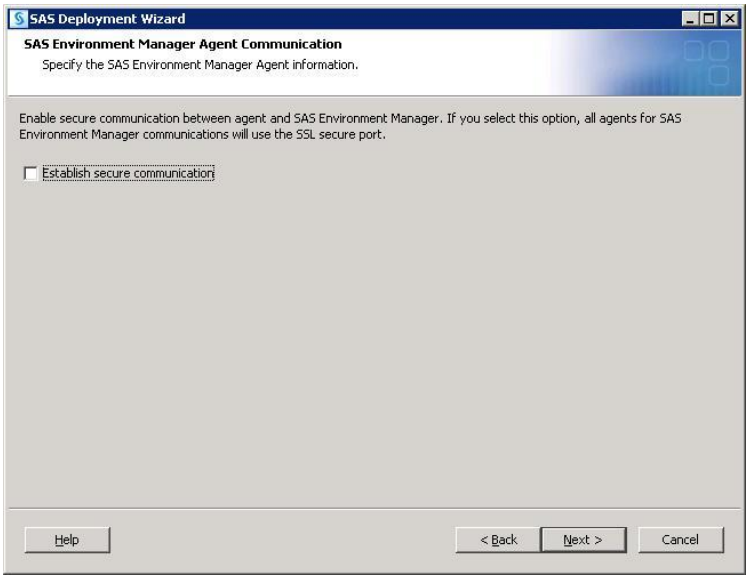


3. A window appears that prompts for the path to the JKS Keystore file and the password for the keystore. You should have this information, and the keystore file's location should have been provided on the pre-installation requirements document (PIRD).

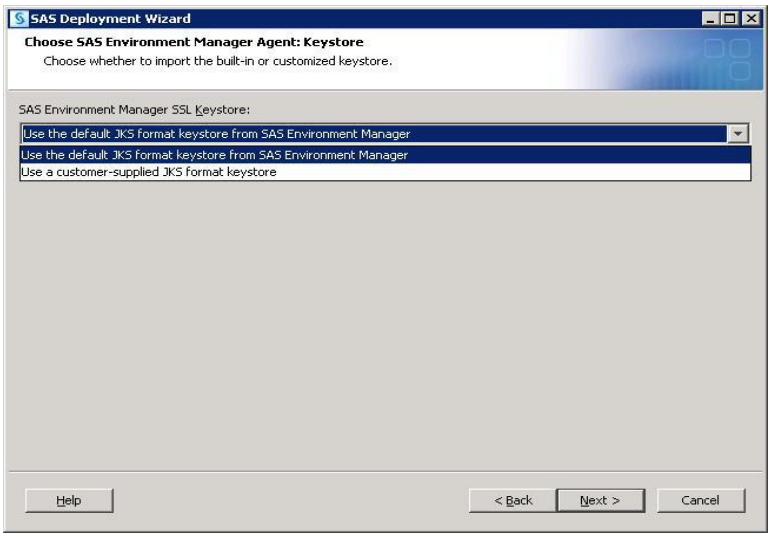


SAS Environment Manager Agent Configuration

1. The SAS Environment Manager agent configuration starts from the following window in SAS Deployment Wizard.



2. Choose **Use the default JKD format keystore from SAS Environment Manager**.



The SAS Environment Manager agent configuration depends only on the SAS Web Application Server's SSL option. If SAS Web Application Server SSL is turned off, the SAS Environment Manager agent will not use secure communication with the SAS Environment Manager server by default. If SAS Application Web Server SSL is turned on, the SAS Environment Manager agent will use secure communication with the SAS Environment Manager server by default.

SAS Post-Configuration

Since we are providing our own certificates, the post-deployment process for SAS Environment Manager consist of the following steps, all documented in *SAS 9.4 Intelligence Platform Installation and Configuration Guide Second Edition*:

1. Disable HTTP for SAS Environment Manager"
2. Change security callback URLs
3. Manually update web.xml
4. Manually update hq-server.conf

SNMP CONFIGURATION

STEP 1: VERIFY SNMP INSTALLATION

1. Verify whether SNMP is installed on your host, by running the following command and looking for the packages listed in the table.

```
[root@myserver ~]# yum list installed | grep snmp
net-snmp.x86_64                    1:5.5-54.el6_7.1        @rhel-x86_64-server-6
net-snmp-libs.x86_64               1:5.5-54.el6_7.1        @rhel-x86_64-server-6
net-snmp-utils.x86_64              1:5.5-54.el6_7.1        @rhel-x86_64-server-6
php-snmp.x86_64                    5.3.3-46.el6_6          @rhel-x86_64-server-optional-6
[root@myserver ~]#
```

Package	Provides
net-snmp	The SNMP agent daemon and documentation. This package is required for exporting performance data.

net-snmp-libs	The `netsnmp` library and the bundled management information bases (MIBs). This package is required for exporting performance data.
net-snmp-utils	SNMP clients such as `snmpget` and `snmpwalk`. This package is required in order to query a system's performance data over SNMP.

2. If SNMP is not installed, run the following command to install it.

```
[root@myserver ~]# yum install net-snmp net-snmp-libs net-snmp-utils
```

STEP 2: CONFIGURE A LOCAL SNMP TRAP RECEIVER FOR TESTING

1. Redirect the SNMP trap log against a specific file. Modify the `smnptrapd.conf` file, add these two lines in the configuration file, located in `/etc/snmp`:

   ```
   authCommunity log,execute,net public
   logOption f /tmp/snmptraps.log
   ```

2. Restart the SNMP trap daemon by issuing one of these commands:

   `/etc/init.d/snmptrapd restart`
   or
   `service snmptrapd start`

3. Restart the SNMP daemon by issuing one of these commands:

   `/etc/init.d/snmpd restart`
   or
   `service snmpd start`

4. After starting/restarting the SNMP daemons, you will see these messages in the log files:
   - in the redirected `/tmp/snmptraps.log`

```
[root@myserver ~]# cat /tmp/snmptraps.log
NET-SNMP version 5.5
[root@myserver ~]#
```

   - in the default location, `/var/log/messages`

```
[root@myserver ~]# tail -2 /var/log/messages
2015-11-11T14:51:01.347282-05:00 sasserver02 snmptrapd[26944]: NET-SNMP version 5.5
2015-11-11T14:51:14.036894-05:00 sasserver02 snmpd[27427]: NET-SNMP version 5.5
[root@myserver ~]#
```

   Note: The SNMP trap log is supposed to be redirected against the `/tmp/snmptraps.log` file.

   If it is not redirected, verify the SELinux settings. To allow the SNMP trap log file redirection, SELinux must be set to `permissive`. To read the current SELinux settings, use the `getenforce` command.
   If the SELinux setting is `Enforcing` instead of `Permissive`, you can change this setting by performing one of these steps:

   - Change SELinux temporarily, only for the current session:

     Use the command `setenforce 0` to set SELinux to `Permissive`

```
[root@myserver ~]# getenforce
Enforcing
[root@myserver ~]#
[root@myserver ~]# setenforce 0
[root@myserver ~]#
[root@myserver ~]# getenforce
Permissive
[root@myserver ~]#
```

Note: Specify `setenforce 1` to set SELinux to `Enforcing`
The SELinux setting will be set for the current session only. After the host reboots, the SELinux settings will return to the defaults.

- Change the SELinux setting permanently:

  Modify the SELinux configuration file `/etc/selinux/config`. Change the value of the `SELINUX=` parameter to `permissive`.
  Save the SELinux configuration file, and then reboot the host.

```
[root@myserver ~]# cat /etc/selinux/config

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
# enforcing - SELinux security policy is enforced.
# permissive - SELinux prints warnings instead of enforcing.
# disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of these two values:
# targeted - Targeted processes are protected,
# mls - Multi Level Security protection.
SELINUXTYPE=targeted

[root@myserver ~]#
```

STEP 3: VERIFY THE SNMP TRAP RECEIVER

1. Verify that the snmpd server is operating correctly by issuing these commands (Note: use `Ctrl-C` to stop the command.):

   ```
   snmptest -v 2c -c public [host FQDN]
   Variable: system.sysDescr.0
   Variable:<Enter>
   ```

```
[root@myserver ~]# snmptest -v 2c -c public myserver.mydomain
Variable: system.sysDescr.0
Variable:
Received Get Response from UDP: [10.96.3.9]:161->[0.0.0.0]
requestid 0x48DFA66B errstat 0x0 errindex 0x0
SNMPv2-MIB::sysDescr.0 = STRING: Linux myserver 2.6.32-358.6.2.el6.x86_64 #1 SMP Tue May 14
15:48:21 EDT 2013 x86_64
Variable:
[root@myserver ~]#
```

2. Create the UCD-TRAP-TEST-MIB Management Information Base (MIB) file. This file is not defined by default. You must create this file: `/usr/share/snmp/mibs/UCD-TRAP-TEST-MIB.txt`. If you do not create this file, you will receive an error message when you run the test in the following steps. Create the file as follows:

```
[root@myserver ~]# cat /usr/share/snmp/mibs/UCD-TRAP-TEST-MIB.txt
UCD-TRAP-TEST-MIB DEFINITIONS ::= BEGIN
      IMPORTS ucdExperimental FROM UCD-SNMP-MIB;


demotraps OBJECT IDENTIFIER ::= { ucdExperimental 990 }


demoTrap TRAP-TYPE
      ENTERPRISE demotraps
      VARIABLES { sysLocation }
      DESCRIPTION "An example of an SMIv1 trap"
      ::= 17


END
[root@myserver ~]#
```

3. Issue a simple and local `snmptrap` command.

```
snmptrap -v 1 -c public [host FQDN] UCD-TRAP-TEST-MIB::demotraps "" 6
17 "" SNMPv2-MIB::sysLocation.0 s "snmp test string"
```

```
[root@myserver ~]# snmptrap -v 1 -c public myserver.mydomain UCD-TRAP-TEST-MIB::demotraps "" 6 17
"" SNMPv2-MIB::sysLocation.0 s "snmp test string"
[root@myserver ~]#
```

4. Verify that the following log entries have been written:
    - in the redirected location `/tmp/snmptraps.log`:

```
[root@myserver ~]# cat /tmp/snmptraps.log
NET-SNMP version 5.5
2015-11-11 15:29:26 myserver.mydomain [10.96.3.9] (via UDP: [10.96.3.9]:49172->[10.96.3.9]) TRAP,
SNMP v1, community public
        UCD-SNMP-MIB::ucdExperimental.990 Enterprise Specific Trap (17) Uptime: 5 days,
6:55:46.99
        SNMPv2-MIB::sysLocation.0 = STRING: snmp test string
[root@myserver ~]#
```

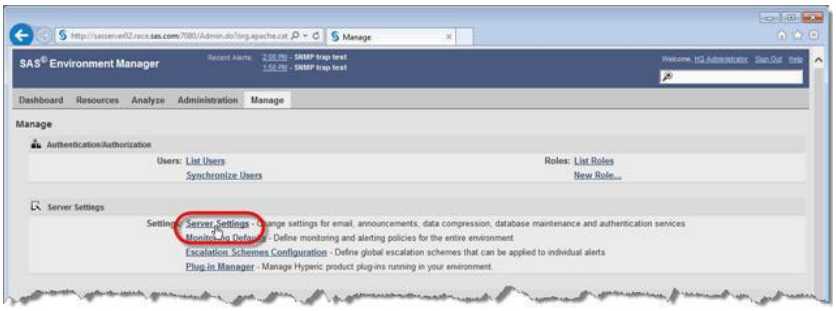
    - in the default location `/var/log/messages`

```
[root@myserver ~]# tail -1 /var/log/messages
2015-11-11T15:29:26.756754-05:00 myserver snmptrapd[26944]: 2015-11-11 15:29:26 myserver.mydomain
[10.96.3.9] (via UDP: [10.96.3.9]:49172->[10.96.3.9]) TRAP, SNMP v1, community public#012#011UCD-
SNMP-MIB::ucdExperimental.990 Enterprise Specific Trap (17) Uptime: 5 days,
6:55:46.99#012#011SNMPv2-MIB::sysLocation.0 = STRING: snmp test string
[root@myserver ~]#
```

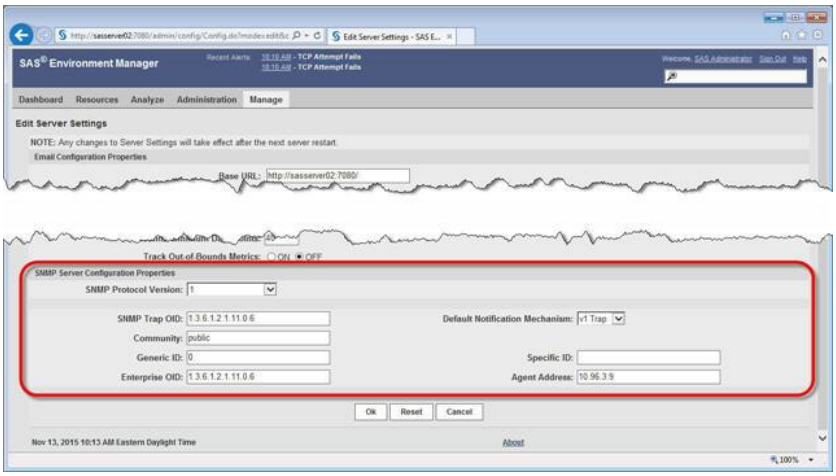
STEP 4: ENABLE SNMP TRAP SENDING IN SAS ENVIRONMENT MANAGER

To enable SNMP notification for SAS Environment Manager alerts, you must first enable SNMP trap sending.

1. Log on to SAS Environment Manager as an administrator and select **Manage ➤ Server settings ➤ Server Settings**.



2. On the **Server Settings** window, scroll to the bottom of the window, and set the following required parameters:



SNMP Protocol Version: 1
SNMP OID: 1.3.6.1.2.1.11.0.6
Community: public (default value)
Generic ID: 0 (zero)
Enterprise OID: 1.3.6.1.2.1.11.0.6
Default Notification Mechanism: v1 Trap (selected from the drop-down list)
Specific ID: (leave blank)
Agent Address: *10.96.3.9* (Your SAS Environment Manager server IP address) [

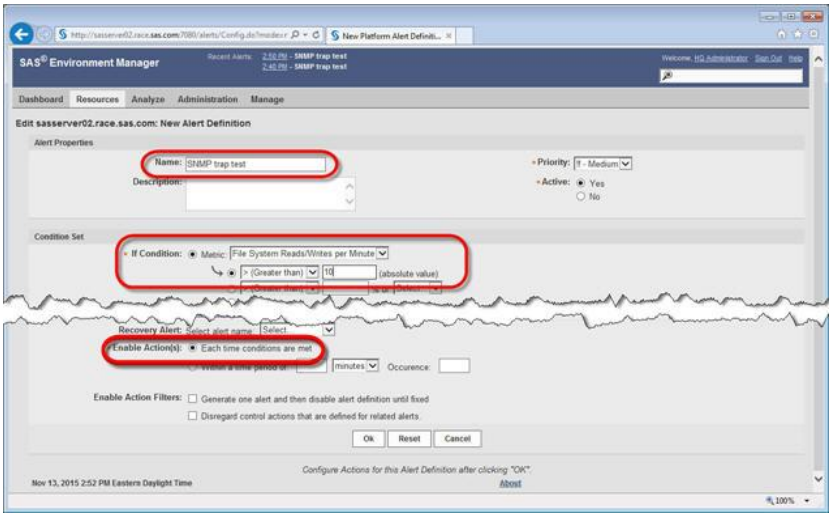
For more detailed information, see the following sources:

- Simple Network Management Protocol, available at https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol
- Object Identifier, available at https://en.wikipedia.org/wiki/Object_identifier
- Object Identifier (OID) Repository, available at http://www.oid-info.com/

STEP 5: CREATE AN SNMP TRAP TEST ALERT IN SAS ENVIRONMENT MANAGER

Next, you must create an alert in SAS Environment Manager to test the SNMP notification.

1. Log on as an administrator then select **Resources ➤ Browse ➤ Platform**.
2. Select the platform where your SAS Environment Manager server is deployed, select the entry for the server, and select **Alert ➤ Configure** to create a new alert.



3. Specify the following values:

   If Condition:

   Metric (selected with the radio button),

   File System Reads/Writes per Minute (selected from the drop-down list)
   Absolute value (selected with the radio button),

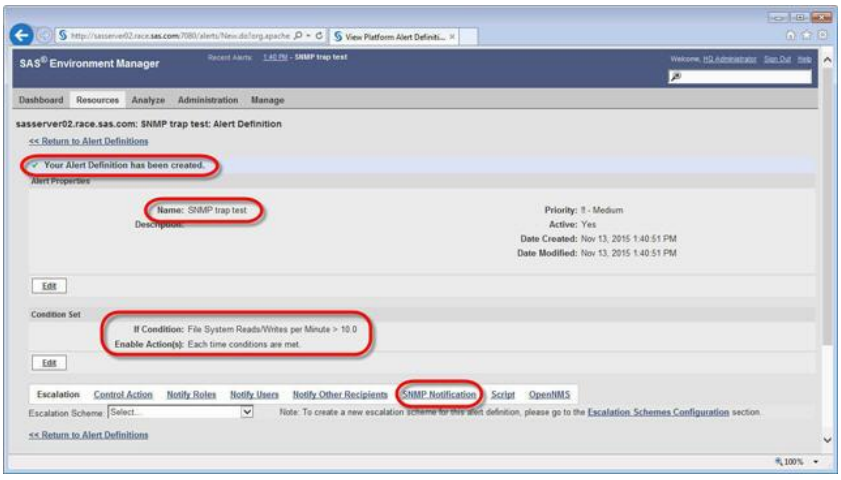
   Greater than (selected from the drop-down list)

   Value: 10 (ten)

   Enable Action(s):

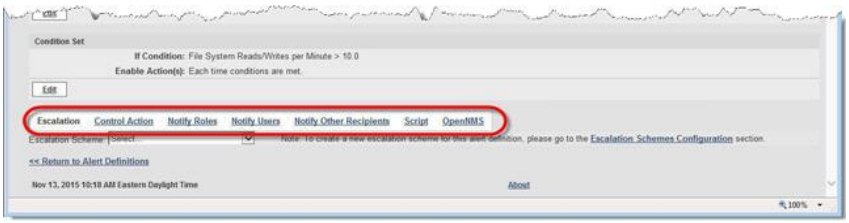
   Each time conditions are met (using the radio button)

4. After the new alert is created, select **SNMP Notification.**



STEP 6: ENABLE SNMP NOTIFICATION ON THE SNMP TRAP TEST ALERT

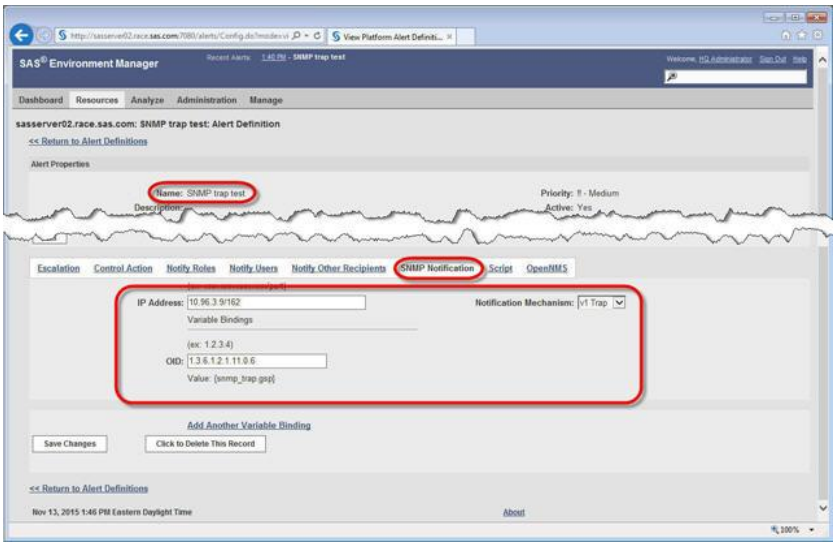
1. If **SNMP Notification** is not available, that indicates that the SNMP server configuration properties were not defined correctly. Go to Step 1, Verify SNMP Installation.



2. If **SNMP Notification** is available, the SNMP server configuration properties were specified correctly.

3. Set the following SNMP notification parameters

   IP Address: *10.96.3.9*/162 (Your SNMP server IP address / SNMP trap port)
   OID: 1.3.6.1.2.1.11.0.6
   Notification Mechanism: v1 Trap (selected from the drop-down list)



STEP 7: ENABLE SNMP NOTIFICATION ON THE SNMP TRAP TEST ALERT

Set your corporate enterprise management tools to read the SAS Environment Manager SNMP notification.

CONCLUSION

This paper discussed three advanced features in SAS Environment Manager. For user management, the model in the third maintenance release of SAS 9.4 solved most of our concerns, and we believe the user

management in SAS Environment Manager is stable now. For SSL configuration, the current implementation in the third maintenance release of SAS 9.4 still has much room for improvement. From the technical perspective, SNMP integration is relatively mature and has standards to follow. The example in this paper helps in educating customers on implementing SNMP integration with SAS Environment Manager.

REFERENCES

SAS Institute Inc. 2015. *What's New in SAS® 9.4,* Cary, NC: SAS Institute Inc. Available at http://supportprod.unx.sas.com/documentation/cdl/en/whatsnew/64788/PDF/default/whatsnew.pdf

SAS Institute Inc. 2015. *SAS® 9.4 Intelligence Platform: Installation and. Configuration,* Cary, NC: SAS Institute Inc. Available at http://support.sas.com/documentation/cdl/en/biig/69172/PDF/default/biig.pdf

SAS Institute Inc. 2015. *SAS® Environment Manager 2.5 User's Guide.* Cary, NC: SAS Institute Inc. Available at http://supportexp.unx.sas.com/documentation/configuration/ebi/evug.pdf

Peters, Amy, Bonham, Bob, and Li, Zhiyong. 2013, "Monitoring 101: New Features in SAS 9.4 for Monitoring Your SAS Intelligence Platform." *Proceedings of the SAS Global Forum 2013 Conference*. Cary, NC: SAS Institute Inc. Available at https://support.sas.com/resources/papers/proceedings13/463-2013.pdf

Li, Zhiyong, and Fernandez, Alec. 2014, "Migrating SAS® Java EE Applications from WebLogic, WebSphere, and JBoss to Pivotal tc Server." *Proceedings of the SAS Global Forum 2014 Conference*. Cary, NC: SAS Institute Inc. Available at http://support.sas.com/resources/papers/proceedings14/SAS357-2014.pdf

Li, Zhiyong, and Thorland, Mike. 2015, "Your Top Ten SAS® Middle-Tier Questions." *Proceedings of the SAS Global Forum 2015 Conference*. Cary, NC: SAS Institute Inc. Available at http://support.sas.com/resources/papers/proceedings15/SAS1904-2015.pdf

CONTACT INFORMATION

Your comments and questions are valued and encouraged. Contact the authors at:

Zhiyong Li
100 SAS Campus Drive
Cary, NC 27513
SAS Institute Inc.
Phone: (919)531-9068
Email: Zhiyong.Li@sas.com
http://www.sas.com

Gilles Chrzaszcz
2001 avenue McGill College, bureau 1800
Montreal, QC H3A 1G1
SAS Institute Inc.
Phone: (438) 289-1673
Email: Gilles.Chrzaszcz@sas.com
http://www.sas.com