IBM Endpoint Manager
Version 9.0

IBM Endpoint Manager for Security and Compliance Analytics Setup Guide

IBM Endpoint Manager
Version 9.0

IBM Endpoint Manager for Security and Compliance Analytics Setup Guide

Note
Before using this information and the product it supports, read the information in "Notices" on page 15.

This edition applies to version 9, release 0, modification level 0 of IBM Endpoint Manager and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Introduction

IBM® Endpoint Manager for Security and Compliance Analytics (SCA) is a web-based application designed to help manage security, vulnerability, and risk assessment. The application archives security and vulnerability compliance check results to identify configuration issues and report levels of compliance toward security configuration goals.

SCA is a component of IBM Endpoint Manager for Security and Compliance, which includes vulnerability detection libraries and technical controls and tools based on industry best practices and standards for endpoint and server security configuration (SCM checklists). The vulnerability detection libraries and the technical controls enable continuous, automated detection and remediation of security configuration issues.

SCA provides report views and tools for managing the vulnerability of SCM checks.

SCA generates the following reports, which can be filtered, sorted, grouped, customized, or exported using any set of Endpoint Manager properties:

- Overviews of Compliance Status, Vulnerabilities and History
- Checklists: Compliance Status and History
- Checks: Compliance Status, Values, and History
- Vulnerabilities: Rollup Status and History
- Vulnerability Results: Detailed Status
- Computers: Compliance Status, Values, Vulnerabilities, and History
- Computer Groups: Compliance Status, Vulnerabilities, and History
- Exceptions: Management, Status, and History

New features

IBM Endpoint Manager for Security and Compliance Analytics version 1.4 includes the following enhancements:

Support for Endpoint Manager data sources on DB2
: You can now connect to the DB2 database that is installed either on a Windows or Linux computer to download raw data that is uploaded by the Endpoint Manager agents.

Lightweight Directory Access Protocol (LDAP) and User auto-provisioning
: You can add, edit, and remove LDAP servers. You can also authenticate users within LDAP groups with the user auto-provisioning feature.

Multiple datasource support
: Gather and present analytics data on more than one data source.

Session timeout
: Administrators can set a time limit for a logged in user who is inactive for some time and edit the login page.

System Requirements

Set up your deployment according to the system requirements to successfully deploy SCA.

Configure your SCA deployment according to the following requirements:

Table 1. Supported components and system requirements to deploy SCA

Components	Requirements
Supported browser versions	• Internet 8.0, 9.0, and 10.0 • Firefox 3 or later versions, including Extended Support Release version 17 • Google Chrome 10+
Supported IBM Endpoint Manager component versions	• Console versions 8.0, 8.1, 8.2, or 9.0 • Web Reports versions 8.0, 8.1, 8.2, or 9.0 • Windows Client versions 8.0, 8.1, 8.2, or 9.0 • UNIX Client versions 8.0, 8.1, 8.2, 9.0
SCA server operating system requirements	• Microsoft Windows Server 2003 • Microsoft Windows Server 2008 • Microsoft Windows Server 2008 R2
SCA database server requirements	Microsoft SQL Server 2005 Service Pack 2 or later
SCA server	You must have Administrator privileges on the target SCA server.
SCA database	You must have dbcreator permissions on the target SCA database server.
IBM Endpoint Manager database user permissions	IBM Endpoint Manager database user permissions
SCM mastheads and Fixlet sites	• You might have earlier BigFix Fixlets, Tivoli Endpoint Manager Fixlets, and custom Fixlets for security compliance in your deployment. These Fixlets continue to function correctly, but only certain Fixlets display within the SCA reports. • To view the current list of SCM content sites that are supported with SCA, see the technote **What SCM content is available for TEM?**.
TEM DB2 permissions	You must have data administration authority (DATAACCESS) to do the following tasks: • Access to create objects • Access to data within a TEM DB2 database

Setup Considerations

During setup, match your optimum deployment size to your hardware specifications. Use the suggestions as general guidance to setup Security and Compliance Analytics.

Consider the requirements of the following servers when you are calculating the data sizing for SCA.

- Security and Compliance Analytics database server
- Security and Compliance Analytics application server

Although you can install the Security and Compliance Analytics server on the same computer as your SQL Server, doing so might affect the performance of the Security and Compliance Analytics application. Carefully manage the SQL Server memory and if necessary, use a dedicated SQL Server computer.

Security and Compliance Analytics database server

The size of the Security and Compliance Analytics database server depends on the following factors.

- The number of computers
- The amount of content that is subscribed onto these computers
- The number of imports that are run

You can add more disk space for future growth of endpoints and more security compliance checks.

- CPU and memory considerations

  A minimum of 2 to 3 GHz CPU with 4 GB RAM is sufficient for hosting a Security and Compliance Analytics database server. The database server would gather analytics data for several hundred Endpoint Manager clients. The requirements scale with the number of computers and compliance checks.

  It is suggested that you add more RAM for the SQL Server as the deployment environment scales up.

  Use the following suggested sizing matrix for your deployment environment.

Table 2. Suggested sizing matrix for SCA deployment environments

Deployment Size (Number of computers)	**Data Size**	**CPU**	**Memory**
1 - 500	0 - 15 GB	quad core	4 GB
500 - 5,000	15 - 25 GB	quad core	8 GB
5,000 - 30,000	25 - 60 GB	quad core	16 GB
30,000 - 100,000	60 - 165 GB	quad core	32 GB
100,000+	165 GB + 1.5 GB for every 1,000 endpoints	2 x quad core	64 GB+

- Disk space considerations and assumptions

  An example deployment size of 30,000 Endpoint Manager Clients that are subscribed to SCM contents must take into account the following disk space considerations and assumptions:

  – A 60 GB of free disk space is needed by the Security and Compliance Analytics database server with 30,000 Endpoint Manager Clients.
  – Add 1.5 GB free disk space for the SCA database server for every 1,000 more clients.
  – The disk space suggestions are based on the following assumptions:
    - Your deployment environment has an average of 2,000 SCM checks and 200 SCM checks per computer

- 2% check result change over each import (daily)
- 5% of the checks have associated exceptions that are managed in Security and Compliance Analytics
- 1% of the measured value change over each import (daily)
- All measured value analyses for all checks are activated
- Your deployment contains one year of archived compliance data (365 imports)

Note: Disk space size is affected by the sum of the following key elements:

(Number of check results and their compliance change over time) + (Number of vulnerability results and their compliance change over time) + (Number of measured values change over time) + (Computer Group * Checks * Number of imports over time) + (Number of exceptions + Number of Measured Values)

Security and Compliance Analytics application server

- A minimum of 3 GB of free disk space is needed by the SCA Server. 10 GB of free disk space can be sufficient for up to 250,000 computers.
- A 2 to 3 GHz CPU Quad-cores with 4 GB RAM free memory space to support 30,0000 computers.

Note: The Security and Compliance Analytics application has a hard limit of 1 GB of memory use and there are up to 4 simultaneous PDF generation processes which would take about 1 GB of memory use.

Chapter 2. Installing Security and Compliance Analytics

Before installing SCA, ensure that your system meets all prerequisites as described in Systems Requirements .

Install and configure IBM Endpoint Manager Analytics by completing the following steps:

- Install by using an MSI installer
- Perform initial configuration by using the web interface

Download IBM Endpoint Manager Analytics

To download IBM Endpoint Manager Analytics, perform the following steps:

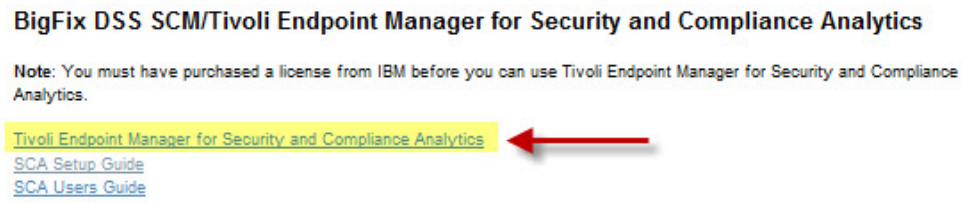
1. In the IBM Endpoint Manager console, add the SCM Reporting masthead.
2. In the Security Configuration domain in the console, open the Configuration Management navigation tree. Click the *Security and Compliance Analytics* dashboard.
3. From the list of supported endpoints, select the target server and click Deploy Installer. An action opens that downloads the SCA software into a Tivoli Endpoint Manager Analytics folder inside the Tivoli Endpoint Manager client folder on that server, for example, `c:\Program Files\BigFix Enterprise\BES Installers\TEMA`).

Note: If you are using the x86 version of a Windows operating system, the path to the install location will be `c:\Program Files (x86)\BigFix Enterprise\BES Installers\TEMA`.

If you are using a version earlier than 8.0 of IBM Endpoint Manager, you will not see the SCA dashboard in your console.

You can manually download the installation files from the following location: http://support.bigfix.com/dss/install/downloaddsssam.html#TEMSCA .

On the download page, scroll down to BigFix DSS SCM/IBM Endpoint Manager for Security and Compliance Analytics and click on the first link.

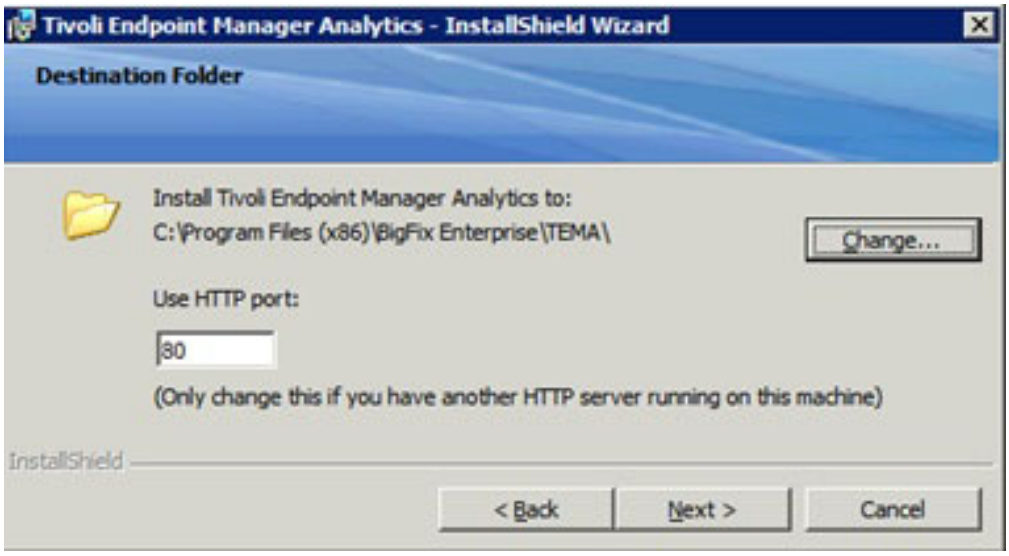


Installing Software

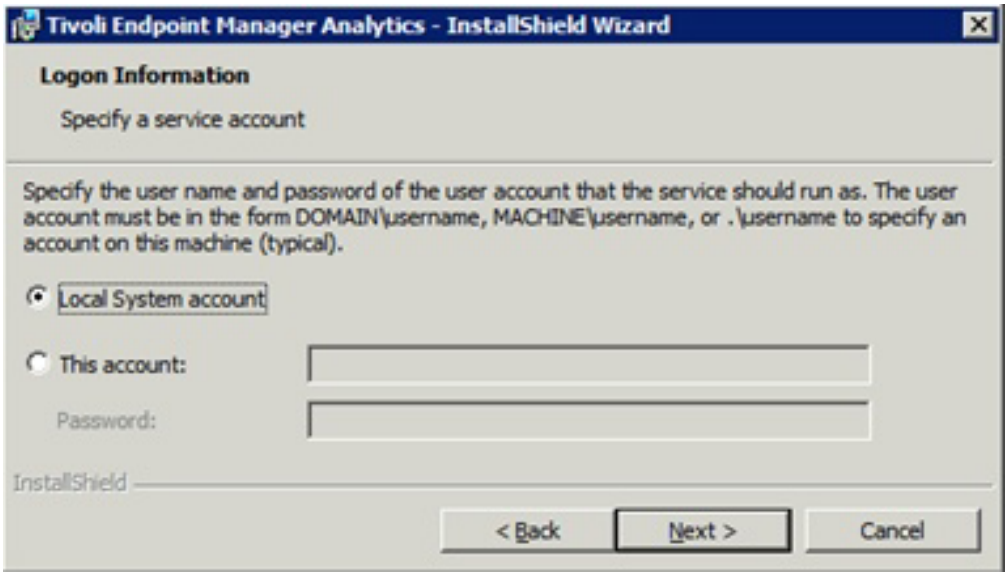
If you install SCA on a Windows system with User Account Control active, you must perform the following steps as an *Administrator*:

In Windows Explorer, open \Program Files\BigFix Enterprise\TEMA\BES Installer\tema_sca_1.3.msi to begin installation.

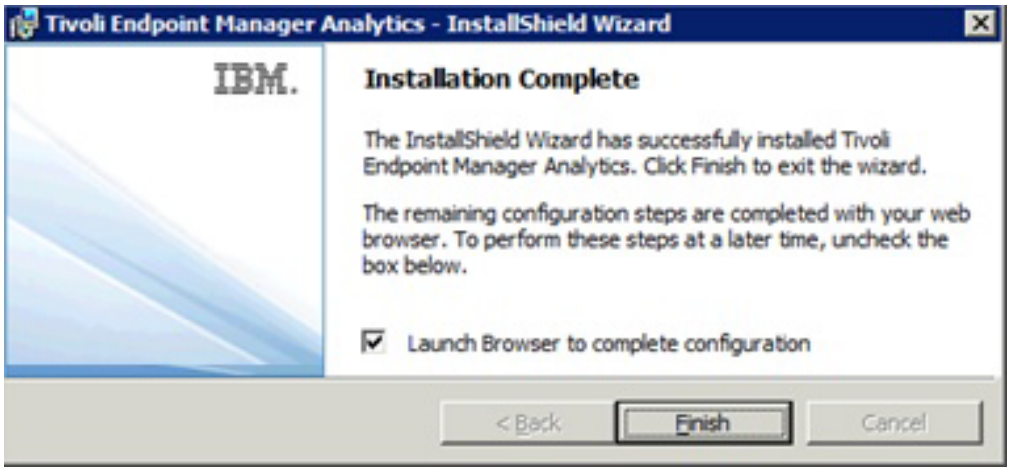
During installation, you can change the installation path as well as the TCP port.



By using the installer, you can specify the user account that runs the Tivoli Endpoint Manager Analytics service. If you configure Tivoli Endpoint Manager Analytics to connect to the SQL Server through a Windows-authenticated user, the Tivoli Endpoint Manager Analytics service must be configured to run as that same user.



After the installation completes, the Tivoli Endpoint Manager Analytics server setup must be completed by using the web interface. The final window of the installer prompts you to launch a web browser to complete the setup.

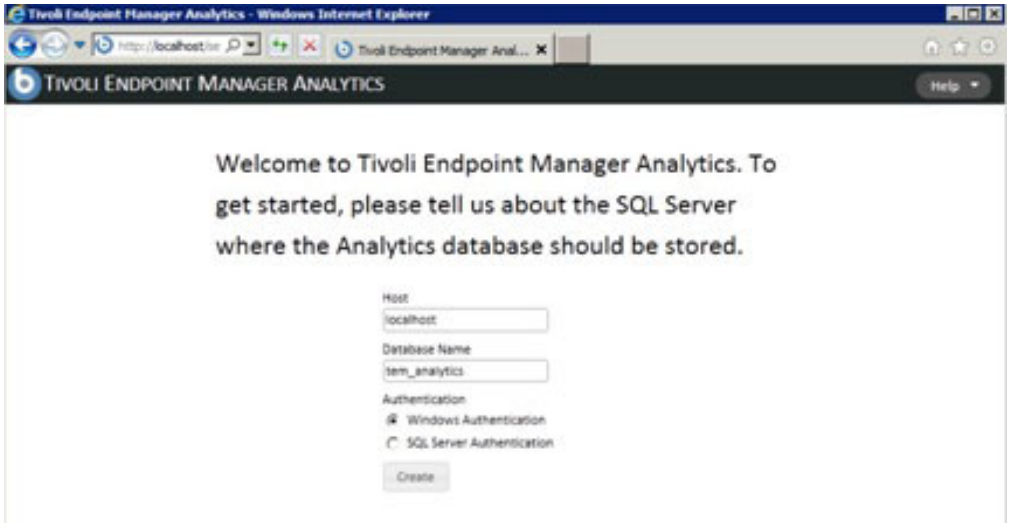


If you configure the system at a later time, you must launch a supported web browser on the Tivoli Endpoint Manager Analytics server and go to http://localhost:<port>, replacing <port> with the port that you configured during installation.

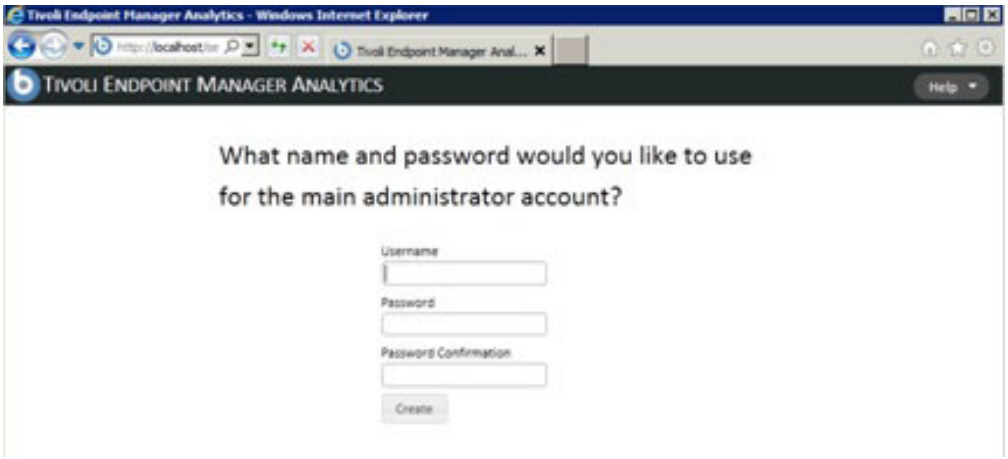
Perform Initial Configuration

To set up the database connection, perform the following steps:

1. Enter the host and database name fields.
2. Select a type of authentication.
3. Click *Create* to create a new administrative user.

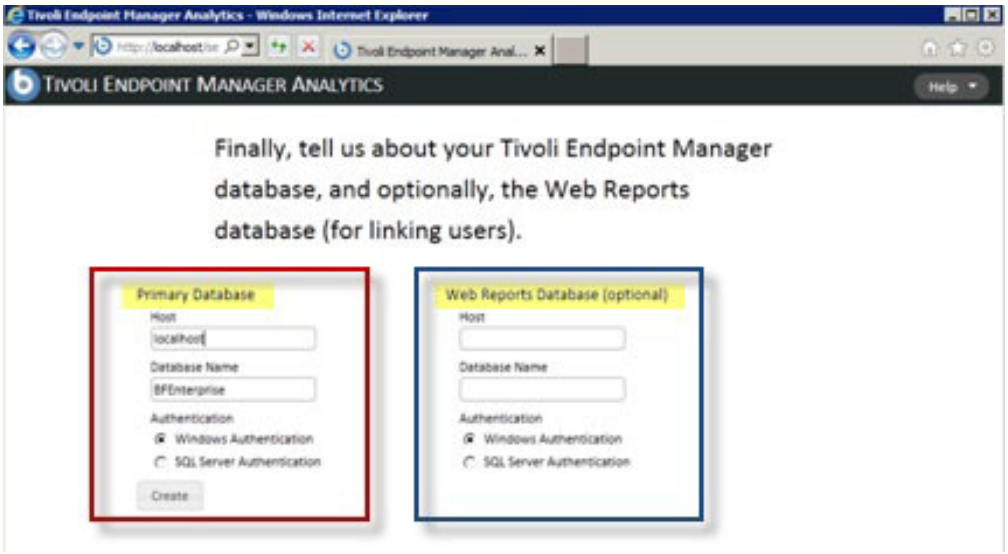


In the next screen, enter a username and password for the new administrator account. Click *Create.*



Next, connect to your IBM Enterprise Manager database. Enter the host, database name, and authentication method for your primary IBM Endpoint Manager database. Click *Create.*

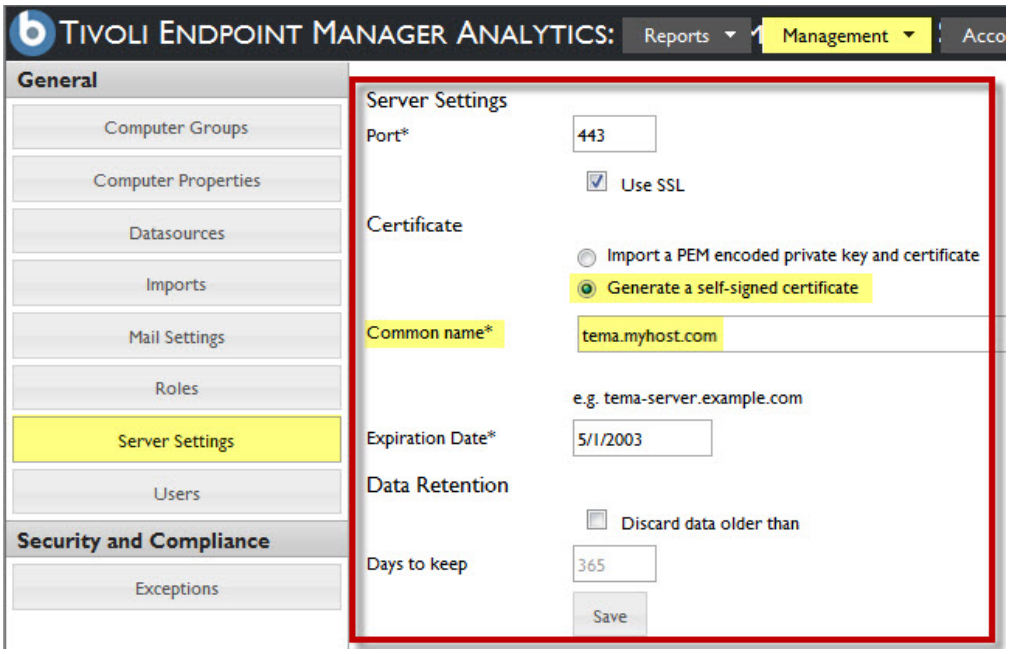
You can also set up a Web Reports database in the fields on the right side of the window.



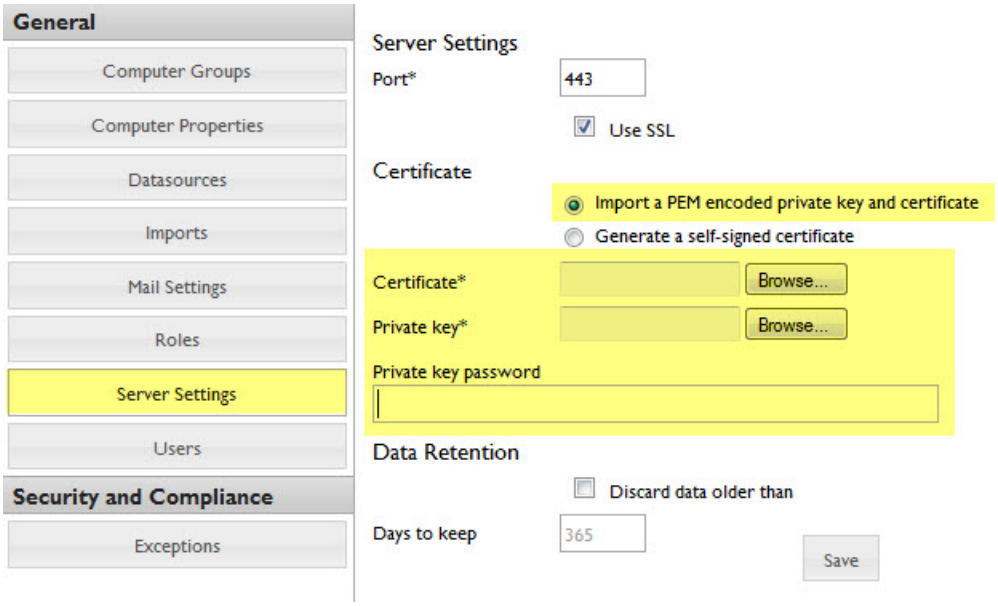
Configure HTTPS

Tivoli Endpoint Manager Analytics administrators can configure SSL and the TCP ports from the Management/Server Settings section of the web interface. When turning on SSL, you can provide a pre-existing private key and certificate or have the system automatically generate a certificate. If you change the port or SSL settings, you must restart the service for the changes to take effect.

If you generate a certificate, you must specify a certificate subject *common name*. The common name must correspond to the DNS name of the Tivoli Endpoint Manger Analytics server.



If you provide a pre-existing private key and certificate, they must be PEM-encoded. If your private key is protected with a password, you must enter it in the *Private key password* field.



Configure the TEMA application server to use LDAP

IBM Endpoint Manager for Security Compliance Security Compliance Analytics 1.4 supports authentication through the Lightweight Directory Access Protocol (LDAP) server. You can add LDAP associations to IBM Endpoint Manager Analytics so you and other users can log in using credentials based on your existing authentication scheme.

To use LDAP for authentication of IBM Endpoint Manager Analytics users, you must do the following steps:

- Add an LDAP server directory
- Link a user to the created directory

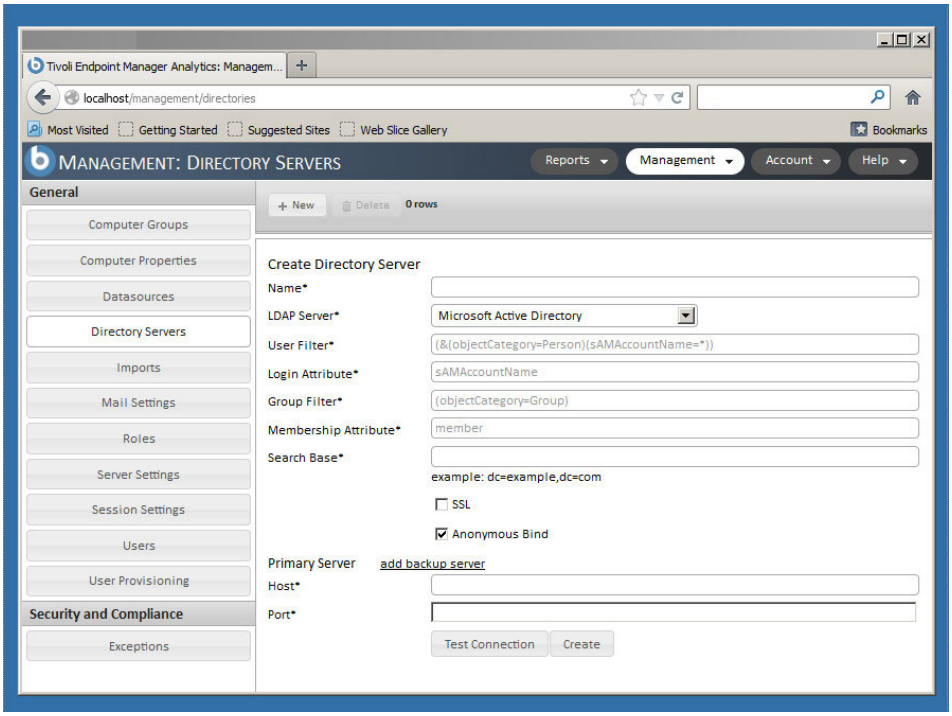
You can also use the user provisioning feature to authenticate LDAP users without creating individual users in the application.

Adding LDAP servers

To use LDAP for authentication of IBM Endpoint Manager Analytics users, you must add a working LDAP directory.

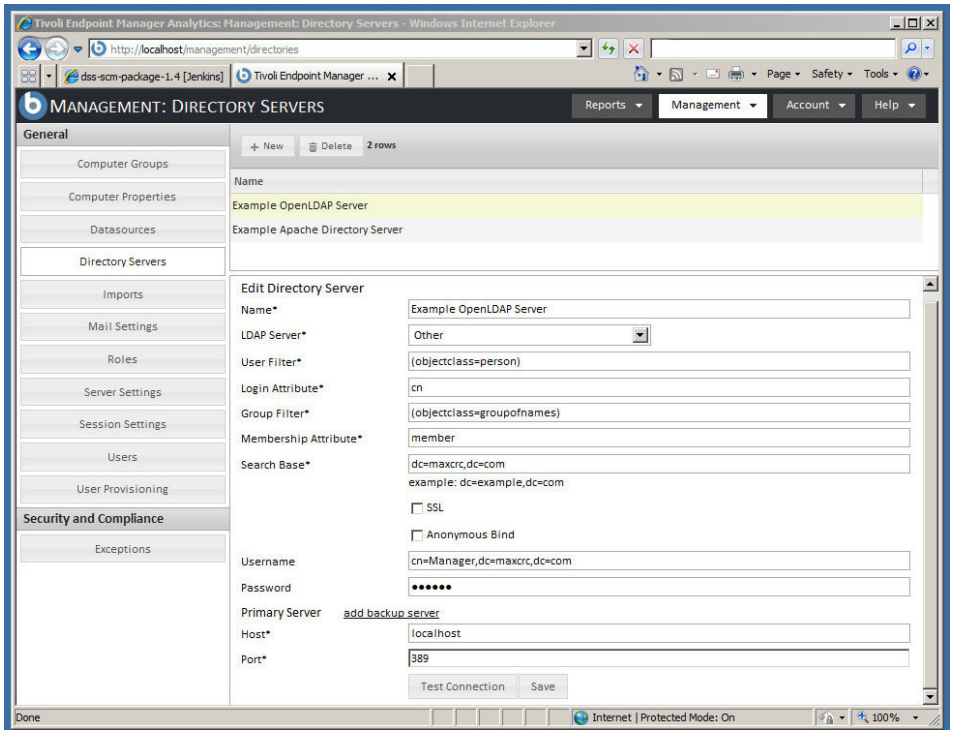
You must be an Administrator to do this task.

1. Log in to the TEMA application server.
2. Go to **Management** > **Directory Servers**.



3. To create an LDAP connection, click **New**.
4. Enter a name for the new directory.
5. Select an LDAP Server for authentication from a list and enter the name of a Search Base
6. If the values of your LDAP server are different from the default, select **Other** from the LDAP Server list.
7. Enter values of filters and attributes of your LDAP server.
8. Enter a name and a password for the authenticated user.
9. If your LDAP server uses Secure Socket Layer protocol, select the **SSL** check box. If you require no user credential, select the **Anonymous Bind** check box.
10. In the Host field, provide the host name on which the LDAP server is installed.
11. Enter the Port.
12. To verify whether all of the provided entries are valid, click **Test Connection**.

13. Click **Create**. You configured a system link to an authentication system.



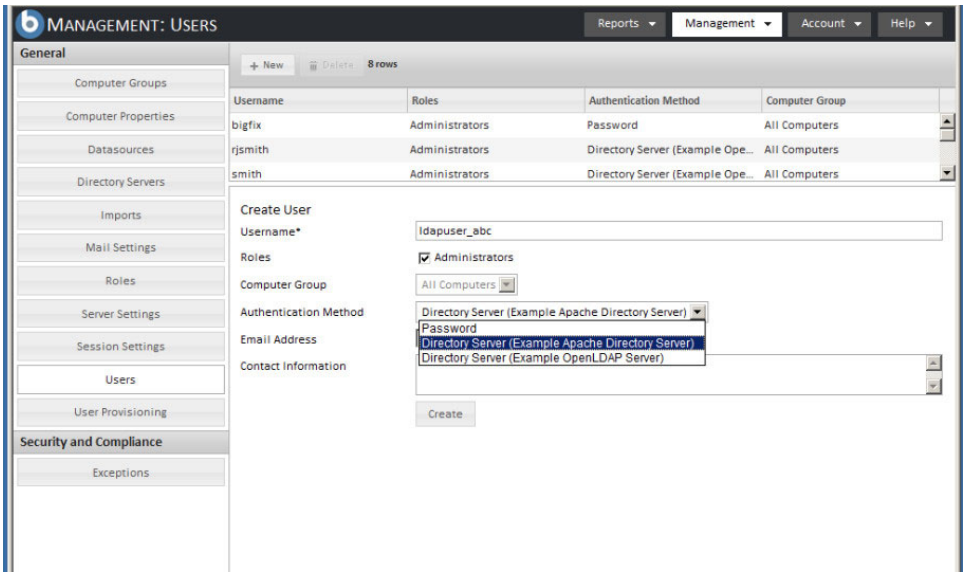
14. To add a backup LDAP server, in the Primary Server tab, click the **Add backup server** link.
    a. Enter the host and IP of the backup LDAP server.
    b. Click **Test Connection** to verify whether all of the provided entries are valid.
    c. Click **Save** to confirm the changes.
15. Optional: To edit the directory, select its name. Click **Save** to confirm the changes.
16. Optional: To delete the created directory, select its name. In the upper left of the window, click **Delete**.

Linking users to directories

To complete an authentication process through LDAP, you must create a user that would link to the created directory.

You must be an Administrator to do this task.

1. Log in to the TEMA application server.
2. Go to **Management** > **Users**.



3. To create a user, click **New**.
4. In the **Username** field, enter the name of an existing user of an LDAP server.
5. From the list, select a Computer Group that the user would be assigned to.
6. From the Authentication Method list, select the name of an LDAP directory.
7. Click **Create**.
8. 8. Optional: To delete the created user, click its name. Then in the upper left of the window, click **Delete**.

To confirm authentication, log in to the Endpoint Manager Analytics server with the credentials.

Authenticating LDAP through user provisioning

You can configure the LDAP group permission to authenticate LDAP users without creating users individually in SCA.

You must configure at least one directory with a working LDAP group in the LDAP server.

1. Log in to the TEMA application server.
2. Go to **Management** > **User Provisioning**.
3. To create a user, click **New**.
4. In the **Group Names** field, type the name of an existing group of an LDAP server.
5. From the list, select a Computer Group that the TEMA would grant for authentication.
6. From the **Roles** field, click one or more roles that the group users granted for access permission.
7. From the **Computer Group** field, select a computer group that the group users would be assigned to.
8. Click **Create**.

To confirm authentication, log in to the Endpoint Manager Analytics server with user within the LDAP group you created.

Appendix. Support

For more information about this product, see the following resources:

- IBM Endpoint Manager Support site
- IBM Endpoint Manager wiki
- Knowledge Base
- Forums and Communities

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web

sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the “Web at Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Printed in USA