IBM Internet Security Systems

SiteProtector System Two-Factor Authentication API Guide

IBM Internet Security Systems

SiteProtector System Two-Factor Authentication API Guide

Copyright Statement

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America.

Trademarks and disclaimer

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. ADDME, Ahead of the threat, BlackICE, Internet Scanner, Proventia, RealSecure, SecurePartner, SecurityFusion, SiteProtector, System Scanner, Virtual Patch, X-Force and X-Press Update are trademarks or registered trademarks of Internet Security Systems, Inc. in the United States, other countries, or both. Internet Security Systems, Inc. is a wholly-owned subsidiary of International Business Machines Corporation.

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

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

Disclaimer: The information contained in this document may change without notice, and may have been altered or changed if you have received it from a source other than IBM Internet Security Systems (IBM ISS). Use of this information constitutes acceptance for use in an "AS IS" condition, without warranties of any kind, and any use of this information is at the user's own risk. IBM Internet Security Systems disclaims all warranties, either expressed or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall IBM ISS be liable for any damages whatsoever, including direct, indirect, incidental, consequential or special damages, arising from the use or dissemination hereof, even if IBM Internet Security Systems has been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages, so the foregoing limitation may not apply.

Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by IBM Internet Security Systems. The views and opinions of authors expressed herein do not necessarily state or reflect those of IBM Internet Security Systems, and shall not be used for advertising or product endorsement purposes.

Links and addresses to Internet resources are inspected thoroughly prior to release, but the ever-changing nature of the Internet prevents IBM Internet Security Systems, Inc. from guaranteeing the content or existence of the resource. When possible, the reference contains alternate sites or keywords that could be used to acquire the information by other methods. If you find a broken or inappropriate link, please send an e-mail with the topic name, link, and its behavior to mailto://support@iss.net.

Overview

The SiteProtector two-factor authentication feature provides a plug-in interface that supports any authentication software you use. This document provides information for helping you determine the best authentication plug-in interface for your network, and provides sample code for creating your authentication.xml files.

Important requirement

To use this feature, you must create your own authentication XML file ("authentication.xml") and place it in the SiteProtector Application Server\config directory.

RADIUS and LDAP authentication

SiteProtector two-factor authentication provides specific plug-in interfaces for RADIUS and LDAP certificate authentication.

Audience

This document is intended for experienced Java developers. You must also have a working knowledge of SiteProtector.

Restriction

The SiteProtector two-factor authentication feature does not manage user credentials.

Topics

RADIUS protocol plug-in

The RADIUS token protocol allows the SiteProtector server to send user-entered information to another server for verification.

How SiteProtector works with RADIUS

SiteProtector will display a second password field to the user on the Logon to Site window, and then package the information the user enters into a single request, as either a PAP or CHAP password attribute.

SiteProtector relays the information package to the RADIUS authentication server, and the server then either grants or denies access to the user in its next message. SiteProtector treats any subsequent challenges issues by the RADIUS server as deny messages since SiteProtector cannot request more information from the user.

Message-Authenticator attributes sign outgoing messages, and incoming messages with the field are verified, although this verification is not required.

Details

The following table provides the detail descriptions for the RADIUS authentication plugin.

Detail	Default	Description
server	none	Address or name of the server to send RADIUS packets to.
port	1812	Port to send RADIUS packets to.
sharedsecret	none	The RADIUS shared secret between the SiteProtector Application Server and the authentication server.
passwordencryption	PAP	Can be “PAP” or “CHAP.”This is the way the password/token will be encoded in RADIUS packets.
username	none	If the user’s name must be modified from how it was typed for the RADIUS server to accept it, make a template here. %USER% and %DOMAIN% will be filled in with the appropriate data. Default is not to do anything. **Example:** %USER%@ %DOMAIN%.com

Detail	Default	Description
timeout	3000	The number of milliseconds to wait for a response before retrying a send or quitting. Increase if RADIUS server is frequently overloaded or is far away.
retries	2	RADIUS packets run on UDP and can be dropped from the network. Two retries means three total attempts before rejecting the authentication.

Example code

Use the code in the example below to set up a RADIUS authentication.xml file on your system.

```
<?xmlversion="1.0" encoding="UTF-8" ?>
<SiteProtectorAuthentication>

 <AuthenticationConfiguration>

  <name>RADIUS Token Authentication</name>

<!-- Make sure to remove line breaks added by page formatting -->

<type>net.iss.rssp.security.auth.plugin.RadiusAuthenticationPlugin</type>

  <primary>true</primary>

 <message>Log in using your PIN plus the value on your token.</message>

  <permissions>
   <ALLUSERS/>
  </permissions>

  <detail attribute="server"
value="radius_server_name_or_address"/>

<!-- see your property encryption documentation for information about how
to enter sharedsecret value -->

  <detail attribute="sharedsecret">
  <encrypted-file>authentication_properties</encrypted-file>
  <keyname>radius.sharedsecret</keyname>
  </detail>
  <detail attribute="passwordencryption" value="PAP"/>
  <detail attribute="username" value="%DOMAIN%\%USER%"/>
  <detail attribute="timeout" value="3000"/>
  <detail attribute="retries" value="2"/>

  <!-- fields 0 (username) and 1 (password) are inferred when
parsing the file, they can be manually defined in order to change the
prompt -->
  <field id="2" type="password" prompt="Token"/>

 </AuthenticationConfiguration>

</SiteProtectorAuthentication>
```

For instructions to encrypt properties, please see “Encrypting sensitive property” on page 9.

Certificate and smart card authentication plug-in

SiteProtector can be configured to verify that a user has a private key, which corresponds to a public certificate that is also submitted with the login attempt.

SiteProtector can allow a user to select a private key from a certificate store or from a smart card. The SiteProtector server generates a random challenge that the client signs and returns with the public certificate.

How the plug-in is chosen

The plug-in for certificate and smart card authentication is chosen based on the way the certificate-to-user name mapping should be done.

- For LDAP, a Windows domain controller can be used, and may possibly contain the certificate mappings already.
- If the controller does not contain the certificate mappings, then a new directory can be created and the certificates can be manually imported into it.

Smart card PKCS#11 library requirement

The smart card log in procedure requires additional configuration on the SiteProtector Console. The Console must have the filename of a properly configured PKCS#11 library. This PKCS#11 library is provided by the hardware vendor and may be different for each Console.

LDAP with user password certificate plug-in

The LDAP with user password plug-in requires the user to log in using both his username and password, and also requires the certificate or smart card.

How SiteProtector works with LDAP

SiteProtector searches the configured directory for certificates that are associated with the user. If any certificates successfully validate the signature for the challenge provided, then the authentication is successful.

If a certificate’s signature is updated, or the certificate is otherwise altered, but the key has not changed from the certificate enrolled in the directory, then this authentication mechanism will continue to work.

Details

The following table provides the detail descriptions for the LDAP with user password certificate authentication plug-in.

Detail	Default	Description
server	none	The URL of the LDAP or AD server, including “ldap://” or “ldaps://”, port number, and the part of the directory needed to log in to. **Examples:** ldap://servername:389/ dc=testsite,dc=com ldaps://secure:636/ dc=testsite, dc=com
authType	simple	How to authenticate to the LDAP server. Can be “simple” (clear-text password) or other SASL types, such as “DIGEST-MD5” or “GSSAPI.”
username	ANONYMOUS	Username for authentication to LDAP server. For AD use “domain\username” unless it is only an LDAP login account.
password	none	Password for authentication to LDAP server.
searchField	userPrincipalName	Attribute to match username to.
searchTemplate	%USER%@%DOMAIN%	A username will usually need to be formatted in a different way to match correctly. Create a template here. **Examples:** %USER%@%DOMAIN%.com %USER%@testsite.com
certAttribute	userCertificate	The attribute in LDAP where the valid certificates for the user object are stored.
searchLocation	“CN=Users”	Where to search in the LDAP tree.
referral	“follow”	Tell LDAP server that referrals can be followed.

Example code

Use the code in the example below to set up LDAP with user password certificate authentication XML file on your system.

```
<?xmlversion="1.0" encoding="UTF-8" ?>
<SiteProtectorAuthentication>

 <AuthenticationConfiguration>
```

```
  <name>Smartcard<</name>

<type>net.iss.rssp.security.auth.plugin.LdapCertificatePlugin</type>
  <primary>false</primary>

<!-- Make sure to remove line breaks added by page formatting -->

  <message>Log in using your smart card. This will not work if you
haven't yet configured your PKCS#11 dll.</message>
  <challenge>SpOnSubmit</challenge>

  <permissions>
   <ALLUSERS/>
  </permissions>

  <!-- details on how to find and log into the LDAP/AD server -->
  <detail attribute="server"
value="ldap://domain_controller:389/dc=domain,dc=net"/>
  <detail attribute="authType" value="simple"/>
  <detail attribute="username"
value="CN=adamuser,OU=AdamUsers,OU=test,DC=domain,DC=net"/>
  <detail attribute="password" value="password"/>
  <detail attribute="referral" value="follow"/>

  <!-- details on how to query for known good certificates for the
user -->
  <detail attribute="searchField" value="userPrincipalName"/>
  <detail attribute="searchTemplate" value="%USER%@%DOMAIN%.net"/>
  <detail attribute="certAttribute" value="userCertificate"/>
  <detail attribute="searchLocation" value="CN=Users"/>

  <!-- Fields 0 and 1 contain username and password by default,
additionally select a certificate -->
  <field id="2" type="certificate" prompt="Key"/>

 </AuthenticationConfiguration>

</SiteProtectorAuthentication>
```

LDAP without user password plug-in

This plug-in uses only the certificate or smart card. SiteProtector searches the configured directory for the user that the certificate belongs to. The certificate is not examined by SiteProtector and is passed to the directory in binary/serialized form. If the directory responds with a user associated with the certificate, the login proceeds with that user.

Details

The following table provides the detail descriptions for the LDAP authentication plug-in.

Detail	Default	Description
server	none	The URL of the LDAP or AD server, including “ldap://” or “ldaps://”, port number, and the part of the directory needed to log in to. **Examples:** ldap://servername:389/ dc=testsite,dc=com ldaps://secure:636/ dc=testsite, dc=com
authType	simple	How to authenticate to the LDAP server. Can be “simple” (clear-text password) or other SASL types, such as “DIGEST-MD5” or “GSSAPI.”
username	ANONYMOUS	Username for authentication to LDAP server. For AD use “domain\username” unless it is only an LDAP login account.
password	none	Password for authentication to LDAP server.
sidField	objectSid	Attribute where the SID is stored. Default probably works.
certAttribute	userCertificate	The attribute to match the certificate with.
searchLocation	“CN=Users”	Where to search in the LDAP tree.
referral	“follow”	Tell LDAP server that referrals can be followed.

Example code

Use the code in the example below to set up the LDAP without user password authentication.xml file on your system.

```
<?xmlversion="1.0" encoding="UTF-8" ?>
<SiteProtectorAuthentication>

 <AuthenticationConfiguration>

  <name>Smartcard<</name>

<type>net.iss.rssp.security.auth.plugin.LdapCertificateOnlyPlugin</type>
  <primary>false</primary>

<!-- Make sure to remove line breaks added by page formatting -->

  <message>Use only the certificate to log in. Server will look for username mappings.</message>
  <challenge>SpOnSubmit</challenge>
  <doNotCheckPassword/>
```

```
  <permissions>
   <ALLUSERS/>
  </permissions>

  <!-- details on where to find and log into LDAP/AD server -->
  <!-- ldaps uses ssl, add ldap server's certificate to
ISS\JRE1.6.0_03\lib\security\cacerts -->
  <detail attribute="server"
value="ldaps://domain_controller/dc=domain,dc=net"/>
  <detail attribute="authType" value="simple"/>
  <detail attribute="username" value="domain\username"/>
  <detail attribute="password" value="password"/>
  <detail attribute="referral" value="follow"/>

  <!-- details on how to query for the username, using the full
binary certificate -->
  <detail attribute="sidField" value="objectSid"/>
  <detail attribute="certAttribute" value="userCertificate"/>
  <detail attribute="searchLocation" value="CN=Users"/>

  <field id="2" type="certificate" prompt="Key"/>

 </AuthenticationConfiguration>

</SiteProtectorAuthentication>
```

Default password plug-in

SiteProtector comes with a default password plug-in that allows users to log in without entering a second authentication factor.

You may decide to allow some users to access SiteProtector using only a password in case the external RADIUS or LDAP server is unavailable or configured incorrectly in some way.

If a user that is not enrolled in an authentication mechanism requires access to SiteProtector, the user's username or group can be added here for normal password access.

Example code

Use the code in the example below to set up the default password authentication.xml file on your system.

```
<?xmlversion="1.0" encoding="UTF-8" ?>
<SiteProtectorAuthentication>

 <AuthenticationConfiguration>

  <name>Default Password</name>
  <type>net.iss.rssp.security.auth.plugin.PasswordPlugin</type>
  <primary>false</primary>
  <message>Log in using your username and password. Not everyone can
use this method.</message>

  <!-- Only the following users may log in using single factor
username/password authentication -->
  <permissions>
   <spgroup>Administrator</spgroup>
   <ntgroup>AnNtUserGroup</ntgroup>
   <user>Username exactly as you log-in here</user>
  </permissions>
```

```
 </AuthenticationConfiguration>

</SiteProtectorAuthentication>
```

Using multiple plug-ins simultaneously

You can configure multiple plug-ins to work at the same time.

You can include any number of "<AuthenticationConfiguration>" entries in a single SiteProtector authentication.xml file. Your users can select among them on the Console's login dialog window.

Example code

In this example, both "Smart card login" and "Steve has no smart card" are included, which means that only the user "Steve" will be able to authenticate without using a smart card:

```
<?xmlversion="1.0" encoding="UTF-8" ?>
<SiteProtectorAuthentication>
 <AuthenticationConfiguration>
  <name>Smart card login</name>
  <permissions>
   <ALLUSERS/>
  </permissions>

 </AuthenticationConfiguration>

 <AuthenticationConfiguration>
  <name>Steve has no smart card</name>
  <permissions>
   <user>Steve</user>
  </permissions>

 </AuthenticationConfiguration>
</SiteProtectorAuthentication>
```

Encrypting sensitive property

This topic describes how to encrypt property and remove an encrypted property from the system.

About this task

SiteProtector two-factor authentication supports the encrypting of details about the configuration so that sensitive information, such as LDAP passwords or RADIUS shared secrets, is not stored directly in the filesystem, where it could be viewed easily or unintentionally cataloged.

Encrypting property

Procedure

1. Create a blank target file, or use a file that is already being used for this purpose.
2. Open a command prompt to Program Files\ISS\SiteProtector\Application Server\bin.
3. Enter the command `Run "ccengine.bat -encryptproperty <filename> <keyname> <value>"` where *filename* is the file to put the property in, and *keyname* is an identifier that will be used to find the property.

   Important:

   - Double-check to be sure the *filename* file exists.
   - The file you create must go in the \CONFIG directory, unless you are using the absolute path in the authentication.xml file.

   Note: You can use any *keyname*, but make sure you remember it. This name will go in the "keyname" attribute of the authentication.xml file to help find the value.

   Note: The *value* is what should be passed to the authentication plug-in. This value would have appeared in the "value" attribute of the authentication.xml file, but now it does not have to.
4. In the authentication.xml file, change the following:

   ```
   <detail attribute="attribute" value="value">
   ```

   To

   ```
   <detail attribute="attribute" encrypted-file="filename"
   keyname="keyname">
   ```

Removing encrypted property

Procedure

To remove an encrypted property from the system, do one of the following:

- To remove the property entirely, delete the file that contains the encrypted property.
- To remove individual properties without losing everything from the file, use this command:

  Run: "ccengine.bat -encryptproperty <*filename*> <*keyname*>"

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 (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, 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
SiteProtector Project Management
C55A/74KB
6303 Barfield Rd.,
Atlanta, GA 30328
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.

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

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 Copyright and trademark information at www.ibm.com/legal/copytrade.shtml.

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

Other company, product, or service names may be trademarks or service marks of others.

Printed in USA