Contents

Chapter 1: Configuring the Enterprise Management Server for Integrated Windows Authentication

Introduction

Product: CA ControlMinder Premium Edition

Release: All

OS: Windows

This scenario describes how a system or a CA ControlMinder administrator configures the Enterprise Management Server for Integrated Windows Authentication (IWA).

Important! The solution is based on a third-party component from Spnego for Kerberos authentication. For information about the component license agreement and other details, see the Spnego SourceForge web site.

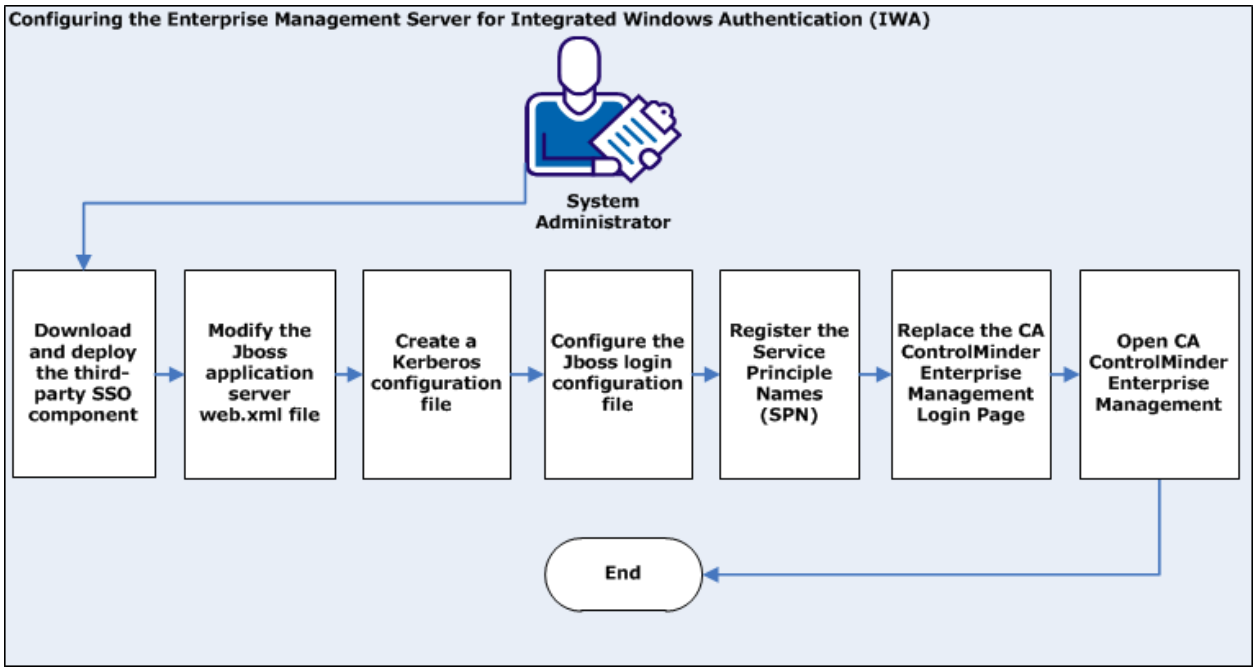
This Knowledge Base Article constitutes a portion of the official CA product documentation for this CA product. This Knowledge Base Article is subject to the following notices (see page 12), terms and conditions.

Configure the Enterprise Management Server for Integrated Windows Authentication

By default, users logs in to CA ControlMinder Enterprise Management by providing their account credentials in the login page. If you specified to use Active Directory as the user store, you can configure the Enterprise Management Server to support Integrated Windows Authentication (IWA) to enable log in to CA ControlMinder Enterprise Management using the users domain account credentials from the user Windows sessions.

Important! Once implemented, IWA is the only authentication method that you can use to log in to CA ControlMinder Enterprise Management.

The following diagram illustrates how you configure the Enterprise Management Server for Integrated Windows Authentication:



Follow these steps:

1. Download and deploy the third-party SSO component (see page 5).

   The third-party component provides SSO capabilities to the Enterprise Management Server.

2. Modify the JBoss application server Web.xml file (see page 6).
3. Create a Kerberos configuration file (see page 8).
4. Configure the JBoss login configuration file (see page 9).
5. Register the Service Principle Names (SPN) (see page 10)

   You register the SPNs to enable the Enterprise Management Server machine to use Kerberos authentication against Active Directory.

6. Replace the CA ControlMinder Enterprise Management login page (see page 10).
7. Open CA ControlMinder Enterprise Management (see page 12).

Download and Deploy the Third-Party SSO Component

To use Windows integrated authentication the Enterprise Management Server uses a third-party component that you download and deploy on the server. The third-party component provides the Enterprise Management Server with single sign on (SSO) capabilities

Follow these steps:

1. On the Enterprise Management Server, open a web browser and navigate to the Sourceforge web site.

   The sourceforge web site opens.

2. Select to download the spnego-r7.jar file and save it to a temporary directory.
3. Copy the spnego-r7.jar file into the following directory, where *JBoss_HOME* indicates the directory where you installed JBoss:

   JBoss_HOME`/server/default/lib`

   You have deployed the spnego single sign on component. Next you configure modify the web.xml file.

Modify the JBoss Application Server web.xml File

The JBoss application server web.xml file defines the parameters and settings of the JBoss application server. You modify the JBoss application server web.xml file to specify the servlet parameters configuration.

Follow these steps:

1. Locate the web.xml file. The file is located by default in the following directory, where *JBoss_HOME* indicates the directory where you installed JBoss:

   JBoss_HOME/server/default/deploy/jboss-web.deployer/conf

2. Open the file for editing then copy the following snippet into the file:

```
<filter>
    <filter-name>SpnegoHttpFilter</filter-name>

<filter-class>net.sourceforge.spnego.SpnegoHttpFilter</filter-clas
s>

    <init-param>
        <param-name>spnego.allow.basic</param-name>
        <param-value>true</param-value>
    </init-param>

    <init-param>
        <param-name>spnego.allow.localhost</param-name>
        <param-value>true</param-value>
    </init-param>

    <init-param>
        <param-name>spnego.allow.unsecure.basic</param-name>
        <param-value>true</param-value>
    </init-param>

    <init-param>
        <param-name>spnego.login.client.module</param-name>
        <param-value>spnego-client</param-value>
    </init-param>

    <init-param>
        <param-name>spnego.krb5.conf</param-name>
        <param-value>krb5.conf</param-value>
    </init-param>

    <init-param>
        <param-name>spnego.login.conf</param-name>
        <param-value>login.conf</param-value>
    </init-param>
```

```
    <init-param>
        <param-name>spnego.preauth.username</param-name>
        <param-value>Administrator</param-value>
    </init-param>

    <init-param>
        <param-name>spnego.preauth.password</param-name>
        <param-value>Z3usP@55</param-value>
    </init-param>

    <init-param>
        <param-name>spnego.login.server.module</param-name>
        <param-value>spnego-server</param-value>
    </init-param>

    <init-param>
        <param-name>spnego.prompt.ntlm</param-name>
        <param-value>true</param-value>
    </init-param>

    <init-param>
        <param-name>spnego.logger.level</param-name>
        <param-value>1</param-value>
    </init-param>
</filter>

<filter-mapping>
    <filter-name>SpnegoHttpFilter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
```

3. Specify an Active Directory administrative account credentials in the spnego.preauth.username and spnego.preauth.password values. For example:

```
<init-param>
        <param-name>spnego.preauth.username</param-name>
        <param-value>Administrator</param-value>
</init-param>
<init-param>
        <param-name>spnego.preauth.password</param-name>
        <param-value>P@ssw0rd</param-value>
</init-param>
```

4. Save and close the file.

   You have modified the web.xml file. Next you create a Kerberos configuration file.

Create a Kerberos Configuration File

The Kerberos configuration file contains information about the Kerberos realms. For each realm you specify the domain and the Kerberos domain controller names (KDC).

Follow these steps:

1. Using a text editor, create a new text file.
2. Open the krb5.conf example file and copy the content into the text file you created.

   Note: You can find the krb5.conf example file in the samples directory in the following path, where *ACSreverInstallDir* is the directory where you installed the Enterprise Management Server:

   ACServerInstallDir/IAMSuite/AccessControl/tools/samples
3. Locate the [realms] section and do the following:
   a. Specify the Active Directory domain name in the default_domain token.
   b. Specify the Kerberos domain name in the kdc token.
4. Save the file as a krb5.conf file under the following directory:

   JBoss_HOME/bin

   You have configured the Kerberos configuration file. Next you configure the login configuration file for JBoss.

Example: The Kerberos configuration file content

The following is a snippet from the Kerberos configuration file, krb5.conf that specifies the Active Directory and Kerberos domain controllers.

```
[libdefaults]
       default_realm=COMPANY.COM
       default_tkt_enctypes = aes128-cts rc4-hmac des3-cbc-sha1
des-cbc-md5 des-cbc-crc
       default_tgs_enctypes = aes128-cts rc4-hmac des3-cbc-sha1
des-cbc-md5 des-cbc-crc
       permitted_enctypes   = aes128-cts rc4-hmac des3-cbc-sha1
des-cbc-md5 des-cbc-crc

[realms]
       COMPANY.COM  = {
              kdc = kdc.company.com
              default_domain = COMPANY.COM
}

[domain_realm]
       .COMPANY.COM = COMPANY.COM
```

The example below indicates that you have specified the Kerberos domain name (company.com) and the default domain name (company.com).

Configure the JBoss Login Configuration File

The JBoss login configuration file controls users login to web applications. You configure the JBoss login configuration file to specify the Spnego Kerberos component.

Follow these steps:

1. On the Enterprise Management Server, browse to the following directory, where *JBoss_HOME* indicates the directory where you installed JBoss:

   JBoss_HOME/server/default/conf

2. Open the login-config.xml file for editing.
3. Copy and paste the following section above the </policy> tag at the bottom of the file:

```
<application-policy name="spnego-client">
   <authentication>
     <login-module
code="com.sun.security.auth.module.Krb5LoginModule"
        flag="required" />
   </authentication>
 </application-policy>

 <application-policy name="spnego-server">
   <authentication>
     <login-module
code="com.sun.security.auth.module.Krb5LoginModule"
        flag="required">
        <module-option name="storeKey">true</module-option>
     </login-module>
   </authentication>
 </application-policy>
```

4. Save and close the file.

   You have configured the JBoss login configuration file. Next you modify the Enterprise Management Server login page.

Register the Service Principle Names (SPN)

A Service Principal Name (SPN) is the name by which a client uniquely identifies an instance of a service. A service instance can have multiple SPNs if there are multiple names that clients can use for authentication. Complete this procedure to enable the Enterprise Management Server machine to use Kerberos authentication against Active Directory.

To register the service principle names of the Enterprise Management Server, use the setspn.exe tool from the Windows Server Tools.

Note: For more information about how to register SPNs, see Registering an SPN on the Spnego SourceForge web site.

Replace the CA ControlMinder Enterprise Management Login Page

You replace the default CA ControlMinder Enterprise Management login page with a login page that supports single sign-on to enable users to log in without providing their domain user accounts.

Follow these steps:

1. Navigate to the samples directory and locate the ac_login_sso.jsp file.

   You can find the ac_login_sso.jsp file in the samples directory in the following path, where *ACSreverInstallDir* is the directory where you installed the Enterprise Management Server:

   ACServerInstallDir/IAMSuite/AccessControl/tools/samples

2. Copy the file to the following directory, where *JBoss_HOME* indicates the directory where you installed JBoss:

   JBoss_HOME/server/default/deploy/IdentityMinder.ear/user_console.war/app

3. Using a web browser, enter the following URL to access the CA Identity Minder Management Console:

   http://*enterprise_host*:port/idmmanage

   The CA Identity Minder Management Console opens.

4. Select Home, Environments, ac-env, Advanced Settings, User Console.

5. Specify the URI of the ac_login_sso.jsp In the Login page to use field:

   app/ac/ac_login_sso.jsp

6. Save the settings and close the CA Identity Minder Management Console.

7. Restart the JBoss application server service.

You have replaced the default CA ControlMinder Enterprise Management login page. Next you can login to CA ControlMinder Enterprise Management.

Example: Enable the CA Identity Minder Management Console

When you install the Enterprise Management Server for the first time, the CA Identity Minder Management Console option is disabled. To enable the CA Identity Minder Management Console, change the default settings.

Follow these steps:

1. Stop JBoss if it is running. Do *one* of the following:
   - From the JBoss job windows, interrupt (Ctrl+C) the process.
   - Stop the JBoss Application Server service from the Services Panel.
2. Navigate to the following directory, where *JBoss_HOME* is the directory where you installed JBoss:

   JBoss_HOME`/server/default/deploy/IdentityMinder.ear/management_console.war/WEB-INF`
3. Open the web.xml file in an editable form. Search for the following section:

   `AccessFilter`
4. In the <param-value> field, change the value to True.
5. Save and close the file.
6. Start the JBoss application server.

   The CA Identity Minder Management Console is enabled.

Open CA ControlMinder Enterprise Management

Once you start CA ControlMinder Enterprise Management you can start the web-based interface from a remote computer using the URL for CA ControlMinder Enterprise Management.

Follow these steps:

1. Open a web browser and enter one of the following URLs, for your host:
   - To use a non-SSL connection, enter the following URL:

     `http://enterprise_host:port/iam/ac`
   - To use an SSL connection, enter the following URL:

     `https://enterprise_host:HTTPSport/iam/ac`

   An Windows authentication screen opens.

   Note: The Windows authentication screen appears if you are not logged in to the domain.
2. Specify your domain user account credentials.

   The CA ControlMinder Enterprise Management welcome screen opens.

Copyright