

CA BEST PRACTICES

CA IT PAM Best Practices for CA EEM

Guidelines for CA EEM Configuration and
Failover

LEGAL NOTICE

This publication is based on current information and resource allocations as of its date of publication and is subject to change or withdrawal by CA at any time without notice. The information in this publication could include typographical errors or technical inaccuracies. CA may make modifications to any CA product, software program, method or procedure described in this publication at any time without notice.

Any reference in this publication to non-CA products and non-CA websites are provided for convenience only and shall not serve as CA's endorsement of such products or websites. Your use of such products, websites, and any information regarding such products or any materials provided with such products or at such websites shall be at your own risk.

Notwithstanding anything in this publication to the contrary, this publication shall not (i) constitute product documentation or specifications under any existing or future written license agreement or services agreement relating to any CA software product, or be subject to any warranty set forth in any such written agreement; (ii) serve to affect the rights and/or obligations of CA or its licensees under any existing or future written license agreement or services agreement relating to any CA software product; or (iii) serve to amend any product documentation or specifications for any CA software product. The development, release and timing of any features or functionality described in this publication remain at CA's sole discretion.

The information in this publication is based upon CA's experiences with the referenced software products in a variety of development and customer environments. Past performance of the software products in such development and customer environments is not indicative of the future performance of such software products in identical, similar or different environments. CA does not warrant that the software products will operate as specifically set forth in this publication. CA will support only the referenced products in accordance with (i) the documentation and specifications provided with the referenced product, and (ii) CA's then-current maintenance and support policy for the referenced product.

Certain information in this publication may outline CA's general product direction. All information in this publication is for your informational purposes only and may not be incorporated into any contract. CA assumes no responsibility for the accuracy or completeness of the information. To the extent permitted by applicable law, CA provides this document "AS IS" without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or non-infringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, lost investment, business interruption, goodwill or lost data, even if CA is expressly advised of the possibility of such damages.

COPYRIGHT LICENSE AND NOTICE:

This publication may contain sample application programming code and/or language which illustrate programming techniques on various operating systems. Notwithstanding anything to the contrary contained in this publication, such sample code does not constitute licensed products or software under any CA license or services agreement. You may copy, modify and use this sample code for the purposes of performing the installation methods and routines described in this document. These samples have not been tested. CA does not make, and you may not rely on, any promise, express or implied, of reliability, serviceability or function of the sample code.

Copyright © [add copyright year] CA. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. Microsoft product screen shots reprinted with permission from Microsoft Corporation.

TITLE AND PUBLICATION DATE:

CA IT PAM Best Practices for CA Embedded Entitlements Manager (CA EEM): Guidelines for EEM Failover Configuration

Publication Date: February 22, 2011

Last Update: February 28, 2011

ACKNOWLEDGEMENTS

Principal Authors and Technical Editors

Yatin Dawada
Terry Pisauro

CA PRODUCT REFERENCES

This document references the following CA products:

- CA IT Process Automation Manager™ (CA IT PAM)
- CA Embedded Entitlements Manager (CA EEM)

FEEDBACK

Please email us at impcdfedback@ca.com to share your feedback on this publication. Please include the title of this publication in the subject of your email response. For technical assistance with a CA product, please contact CA Technical Support at <http://ca.com/support>. For assistance with support specific to Japanese operating systems, please contact CA at <http://www.casupport.jp>.

Contents

| | |
|---|---------------|
| Chapter 1: Introduction | 7 |
| CA EEM High Availability Overview | 7 |
| Users | 8 |
| CA EEM Application Instance | 9 |
| DataStore Replication | 10 |
| CA EEM Server Failover | 11 |
| Resource Kit | 11 |
| Clustering CA IT PAM Orchestrators | 12 |
| Chapter 2: Install and Configure Failover for CA EEM | 13 |
| Overview | 14 |
| Step 1: Install CA EEM on Node1 | 14 |
| Step 2: Define the CA EEM “ITPAM” Application Instance..... | 18 |
| Step 3: Install CA EEM on Node2 | 21 |
| Step 4: Define the CA EEM “ITPAM” Application Instance for Node2..... | 21 |
| Step 5: Configuring CA EEM to Use External Directory | 21 |
| Step 6: Establishing a Trust Relationship Between the CA EEM Servers | 23 |
| Step 7: Define TrustedRoots for CA EEM Servers..... | 26 |
| Step 8: Use the Resource Kit to Configure CA EEM Data Store Replication | 32 |
| Step 9: Install Load Balancer | 37 |
| Step 10: Install CA IT PAM..... | 37 |
| Step 11: Installing the Cluster Node Domain Orchestrator..... | 40 |
| Chapter 3: Synchronize CA EEM Application Instances | 49 |
| Backup and Restore CA EEM Application Instances..... | 49 |
| Updating the CA EEM Backend Server | 52 |
| Chapter 4: Gotchas | 55 |
| Unable to Login to CA EEM Spin | 55 |
| Unable to Login to CA IT PAM Client..... | 56 |
| Removing the CA EEM ITPAM Application Instance | 57 |
| CA EEM Failover Detection | 57 |

Chapter 1: Introduction

CA IT Process Automation Manager (CA IT PAM) is one of many CA products that supports the use of CA Embedded Entitlements Manager (CA EEM) for managing authentication. When CA EEM is used, access policies are created in CA EEM and permissions defined in those policies. CA EEM also allows integration with external directory stores, namely Microsoft Active Directory, Novel eDirectory, SunOne Directory or Custom Mapping Directory, for authentication and authorization.

If you choose to use CA EEM to manage authentication you will also need to consider the following:

- Is CA EEM failover required?
Note: If failover is required and CA EEM is not available, then login to CA IT PAM will be not possible.
- If CA EEM failover is not required, how can the CA EEM Application Instance be backed up so that it can be easily ported to another server?
- How should CA EEM be configured to use an external directory?

This document discusses several Best Practices for configuring CA EEM in a CA IT PAM environment and includes steps on how to:

- Implement CA EEM failover without using a physical cluster, such as Microsoft Cluster
- Setup DataStore Replication using the available resource kit
- Setup CA EEM Server failover using the resource kit
- Configure trusts between CA EEM servers
- Define trustedroots for CA EEM backend servers
- Create a CA IT PAM EEM Application Instance
- Backup a CA EEM Application Instance
- Configure CA EEM to use External Directory

CA EEM High Availability Overview

In CA IT PAM, multiple Orchestrators can be clustered for both failover and load balancing. When one Orchestrator becomes too busy or is unavailable, another Orchestrator can seamlessly take its place, improving the processing efficiency and performance. If CA IT PAM is configured to use CA EEM and the CA EEM server is not available, it will not be possible to login to CA IT PAM client. Since this would have a significant impact, it is important that CA EEM is configured as Highly Available.

When CA EEM is used to manage authentication and authorization for CA IT PAM the following installation options are available:



- Install CA EEM on a separate node or use an existing CA EEM implementation and configure each Orchestrator to use that particular instance of CA EEM
- Install CA EEM on multiple nodes, synchronize CA IT PAM EEM application data and implement CA EEM High Availability.
- Install CA EEM on one node and regularly export CA EEM CA IT PAM application data to a separate node so that, in case of failure, that data can be imported on a different server. This will require changes to the CA IT PAM EEM configuration and a restart of CA IT PAM Orchestrators.

Note that the CA EEM failover method described in this document does not include implementation on a physical cluster, such as a Microsoft Cluster. Although you can use a Microsoft Cluster, you should note that not all CA EEM services can be added as clustered resources. You can define the iGateway service as a cluster resource and also configure the CA EEM datastore replication on all cluster nodes. CA EEM Server failover, however, is not required as that will be provided by the physical cluster itself.

Note: Beginning with r2.2, CA IT PAM allows you to specify multiple EEM Servers as part of the CA IT PAM EEM configuration. If that configuration includes an EEM server that is shared with another EEM application that does not permit multiple EEM servers to be specified, then you should consider installing CA EEM on a physical cluster, such Microsoft Cluster Services.

This document describes following two modes of failover:

- **Data Store replication**

DataStore replication allows application data, such as the itpamadmin and itpamuser details, to be replicated and synchronized between multiple CA EEM Servers. This also applies to Global Users (users extracted from Active Directory) that have been assigned to application groups such as ITPAMAdmin.

- **CA EEM Server failover**

CA EEM Server failover allows a backend server to takeover if the primary CA EEM Server is lost. This process does not require physical cluster.

Users

There are different two different types of “users”:

- **Global users**

Global users are user IDs that can be shared across all applications registered with CA EEM – and are not exclusive to CA IT PAM. Typically, these are users that have been extracted from an external directory, such as Active Directory.

- **Application users**

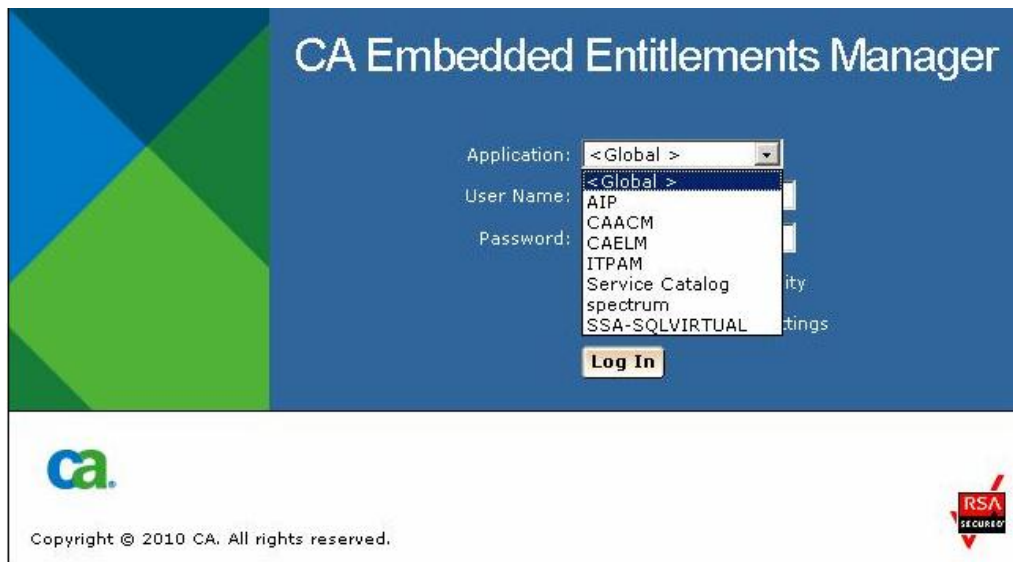
Application users are specific to CA IT PAM. They are not shared across other Application Instances. Application-specific user attributes are defined when creating an Application Instance. You can add a global user to an application group such as ITPamAdmin.

Note: If CA EEM is configured to use an external directory, Application users cannot be added. Application Groups, however, can be added to the Global users.

CA EEM Application Instance

CA EEM provides its services to the applications that are registered with it. When an application registers with CA EEM it creates an “Application Instance” that CA EEM uses to store user details, access policies, calendars and application-specific user groups and folders. In the case of CA IT PAM that Application Instance is called “ITPAM”.

Here you can see examples of several Application Instances registered to CA EEM:



This example depicts the following instances:

- <Global>: Registered when CA EEM is installed.
- CAELM: CA Enterprise Log Manager (CA ELM) Application Instance registered when CA EEM is installed.
- SSA-SQLVIRTUAL: CA Spectrum Service Assurance (CA Spectrum SA) Application Instance Name. The name does vary as it is a configurable option in CA Spectrum SA.
- ITPAM: CA IT PAM Application Instance Name
- Service Catalog: CA Service Catalog Application Instance Name.
- AIP – CA Spectrum Automation Manager Application Instance
- CAACM –CA Application Configuration Manager Instance
- Spectrum – CA Spectrum IM Application Instance

Note: Although CA Service Desk also supports authentication through CA EEM, it maintains its own contact table in its own database and, therefore, does not require Application Instance to be created for it.

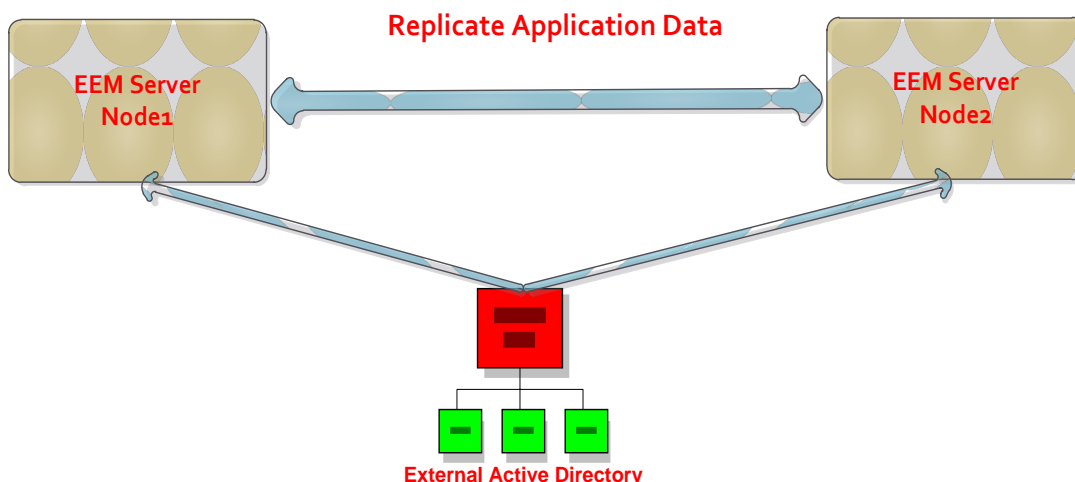
DataStore Replication

DataStore replication allows application data to be synchronized between multiple CA EEM Servers. Application data typically includes policies, application groups, such as ITPAMadmins, and application users, such as ITPAMuser. The application groups and users are different from Global groups and users. Global groups and users, which typically come from Active Directory if CA EEM is configured to use external directories, are **not** replicated. However, if a Global user is part of an application group, such as ITPAMadmins, then that information *will* be replicated.

Since DataStore replication replicates *data that changes* it is imperative that you synchronize the Application Instances *before* setting up Datastore Replication. Information on how to synchronize Application Instances between two CA EEM Servers is provided in Chapter 4: “Synchronizing CA EEM Application Instances” later in this guide. This step will only be necessary if you have decided to setup CA EEM Failover *after* making the security related configuration changes.

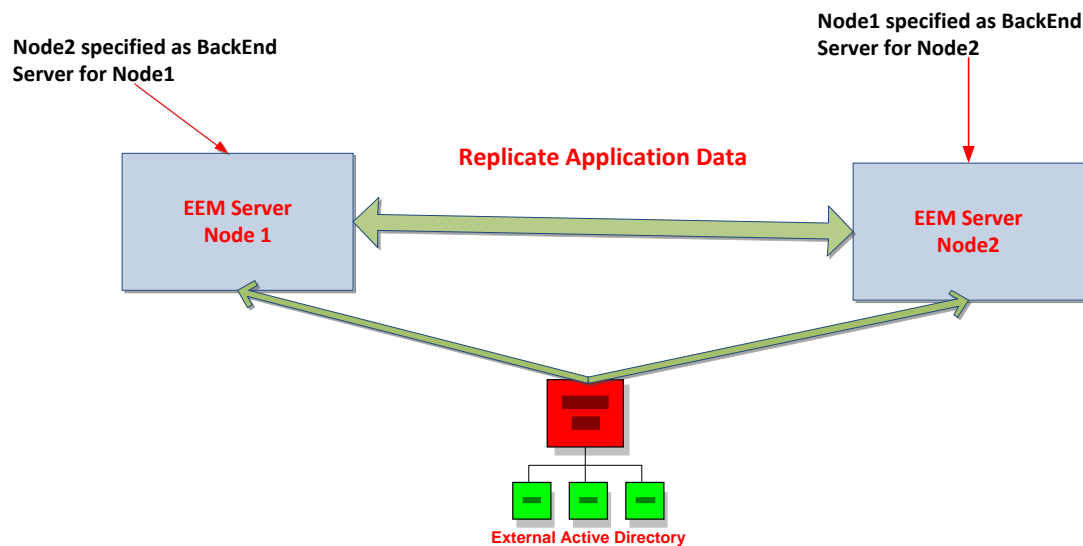
The CA IT PAM EEM Application Instance must already exist on all CA EEM Servers that need to be synchronized. In a typical setup two CA EEM Server nodes should suffice. If the Datastore replication is already enabled and if you create a new Application Instance on one EEM Server, it will automatically create the same application instance on the other EEM Server and replicate its contents

In the following example, two CA EEM Servers are defined for failover. Application data between these two servers will be replicated.



CA EEM Server Failover

If CA EEM Server (Node1 in the following example) is not available, then applications such as CA IT PAM will not function unless CA EEM Server failover has been configured. As part of this configuration, a CA EEM backend server (Node2 in the following example) is specified. When the primary EEM server is not available or if the services are down, EEM requests are automatically routed to the backend server. With the DataStore replication enabled, the application data between the two servers will be synchronized. As a result, when the CA EEM server is switched from the primary to the backend server, the impact on the CA IT PAM application will be minimal.



Resource Kit

A CA EEM Failover Resource Kit is available to simplify the CA EEM configuration required to setup DataStore replication. This kit can be downloaded from the following link:

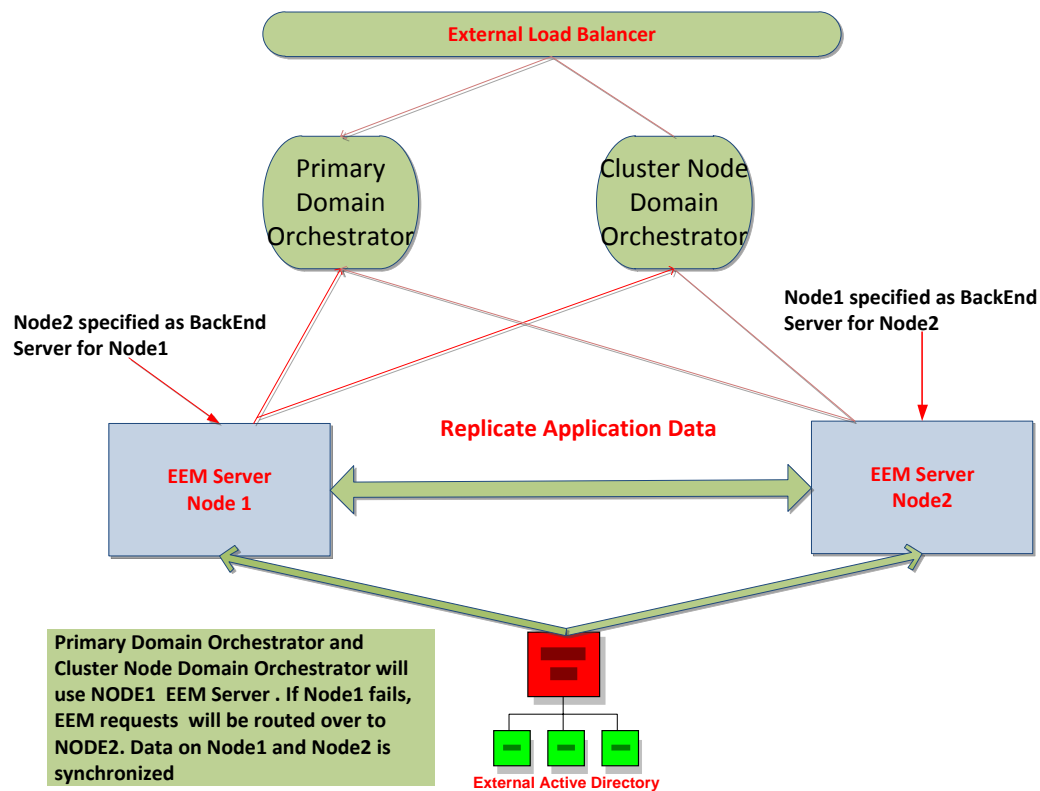
https://support.ca.com/phpdocs/0/common/impcd/r11/Catalyst/doc/EEM_Failover.zip

The CA EEM Failover Resource Kit performs several validation tests, including verifying that the CA EEM Application Instance exists, that CA EEM is installed, that the backend server is pingable, and others. However, it does not define trusts between CA EEM Servers or add trustedroots. These steps need to be done through the CA EEM GUI. Details are provided in Chapter 3.

Clustering CA IT PAM Orchestrators

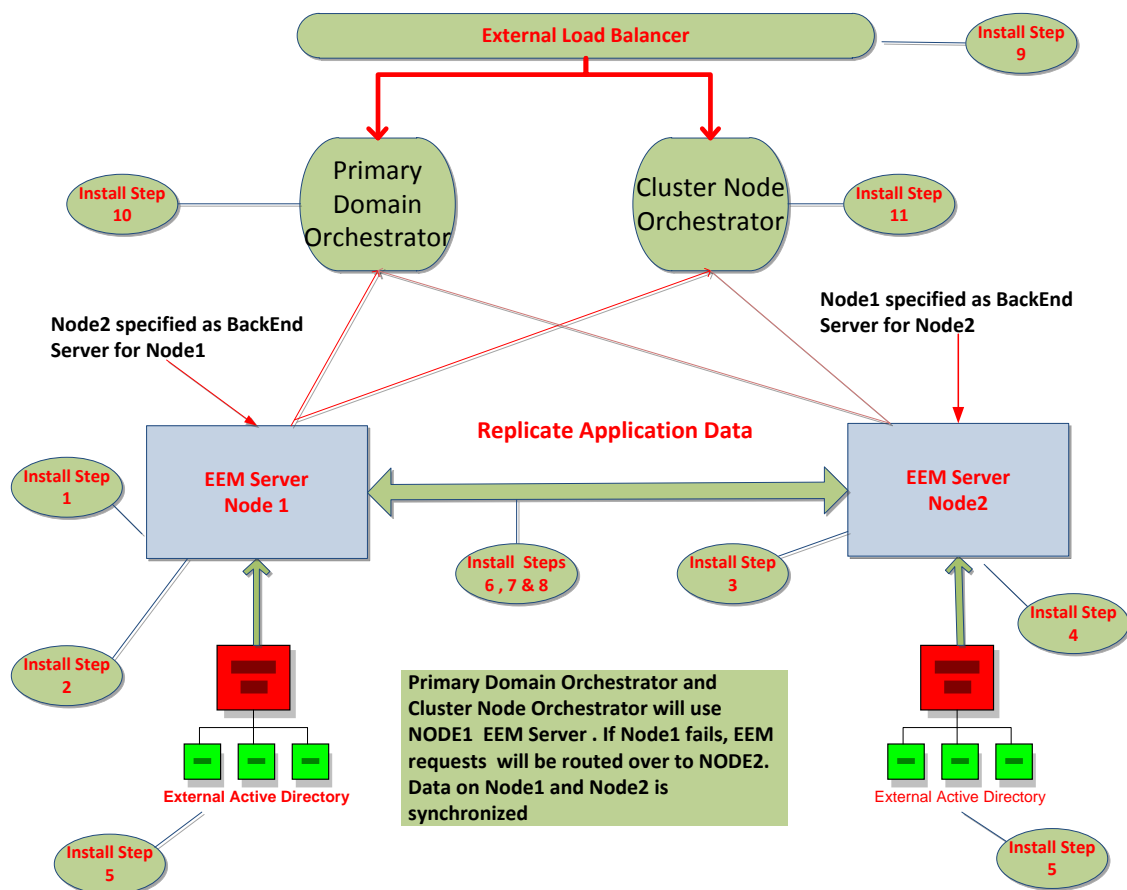
If CA EEM is configured as Highly Available but the application using CA EEM (CA IT PAM, in this case) is not also configured as Highly available, this can have a significant impact as well if the application fails. Following is an example of clustering for CA IT PAM Orchestrators. For more information on installing and configuring an external load balancer, such as Apache, to make CA IT PAM Primary Domain Orchestrators and Cluster Node Domain Orchestrator Highly Available see the *CA IT PAM Best Practices for Continuous and High Availability*. This document is available from the CA IT PAM Best Practices pages (see https://support.ca.com/phpdocs/0/common/impcd/r11/Catalyst/ITPAM_Frame_sc.htm)

In the following example, the Primary Domain Orchestrator and cluster node Domain Orchestrator are configured to use CA EEM Server Node1. If Node1 server is unavailable, CA EEM requests are automatically routed over to the backend CA EEM Server on Node2. Since the CA EEM application data (for example, policies, and the ITPAMAdmins groups) is replicated, the impact on CA IT PAM will be minimal.



Chapter 2: Install and Configure Failover for CA EEM

This chapter outlines the steps required to implement CA EEM Failover. Here you can see the architecture that is used:



Overview

Following is an overview of the procedures that will be used to implement CA EEM Failover:

1. Install CA EEM on Node1
2. Create CA EEM ITPAM Application Instance using the safex command.
3. Install CA EEM on Node2
4. Create CA EEM ITPAM Application Instance using the safex command.
5. Configure CA EEM on both nodes to *Use External Directory*
6. Define EEM Trusts between Node1 and Node2.
7. Configure EEM TrustedRoots for Node1 and Node2.
8. Use the Resource Kit to configure DataStore replication and CA EEM failover.
9. Install Load Balancer
10. Install CA IT PAM Primary Domain Orchestrator
11. Install Cluster Node CA IT PAM Domain Orchestrator

Step 1: Install CA EEM on Node1

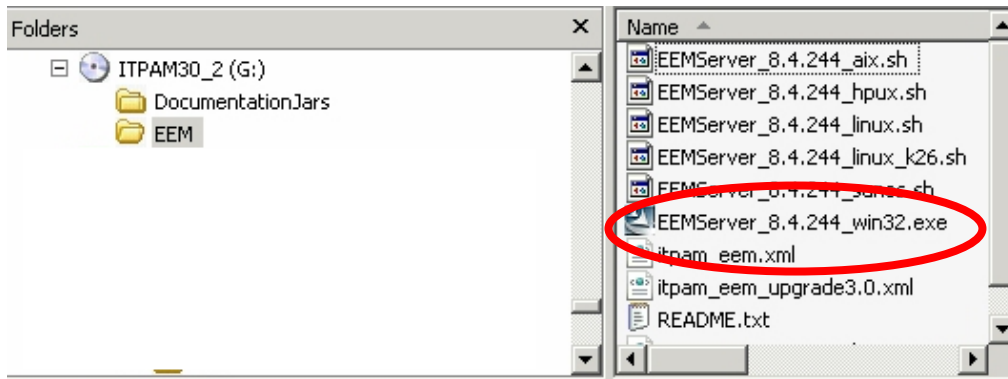
If you intend to setup CA EEM failover or DataStore replication, then you must install CA EEM on two or more servers. It is recommended each of these CA EEM servers be at the same version level and include the same CA EEM Application Instances, such as "ITPAM". For the purposes of our example we are using "Node1" to refer to the Primary node and "Node2" to refer to the backend node.

Note: If you plan to use an existing CA EEM implementation, verify the release level that has been installed. The CA EEM release provided on the CA IT PAM r3.0 installation media is r8.4.244. If you are currently using an earlier version of CA EEM you should consider upgrading to that level. The CA EEM failover tests documented here were based on both CA EEM Servers running at r8.4.244.

If you are installing a new version of CA EEM, then you should first check the CA Support site and download the latest version of CA EEM.

To install CA EEM do the following:

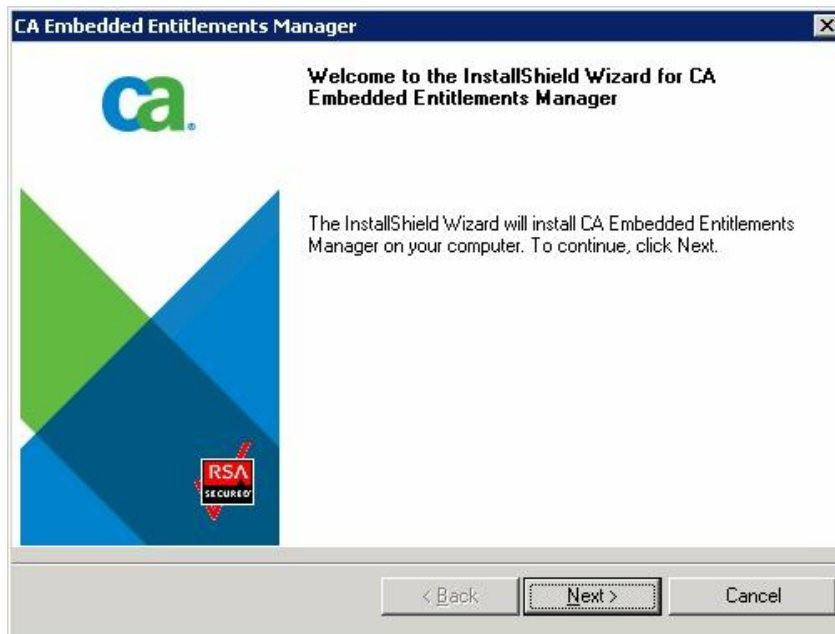
1. Drill into CD2\EEM of the CA IT PAM installation media:



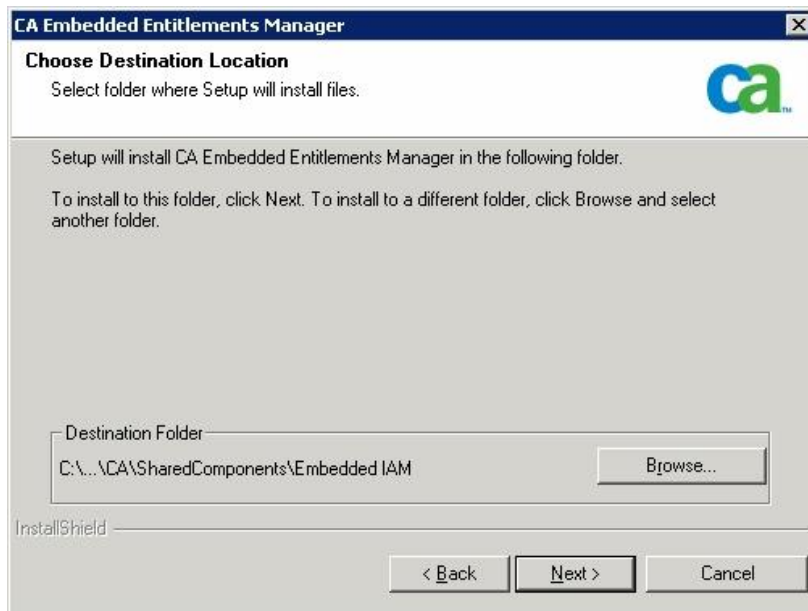
2. Execute the following command

Win32_8.4.244.exe

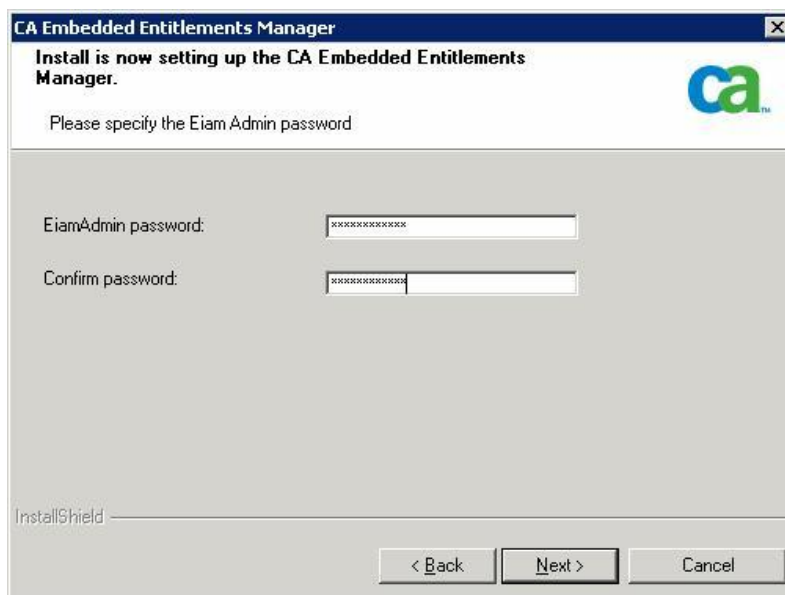
The CA Embedded Entitlements Manager Welcome dialog will appear:



3. Click **Next** to proceed.
4. When prompted to provide the Destination folder, specify the location on the local drive:

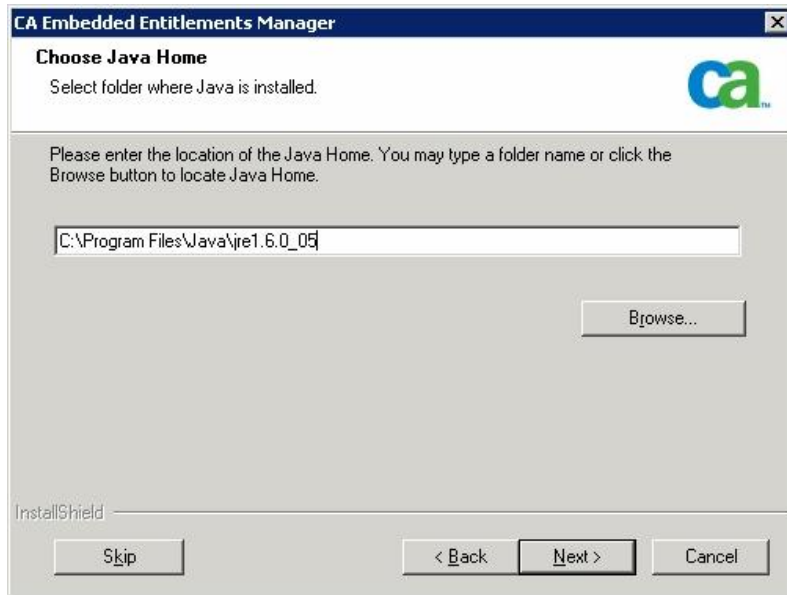


5. Click **Next**



The Eiam Admin password dialog will appear.

6. Provide and confirm the Eiam Admin password and click **Next**.
Important! Ensure that the same EiamAdmin password is specified on **ALL** CA EEM Server Nodes.
7. Provide the JRE location and click **Next**.



CA EEM requires JRE. If JRE is not already installed on the CA EEM node you can download it from the following location:

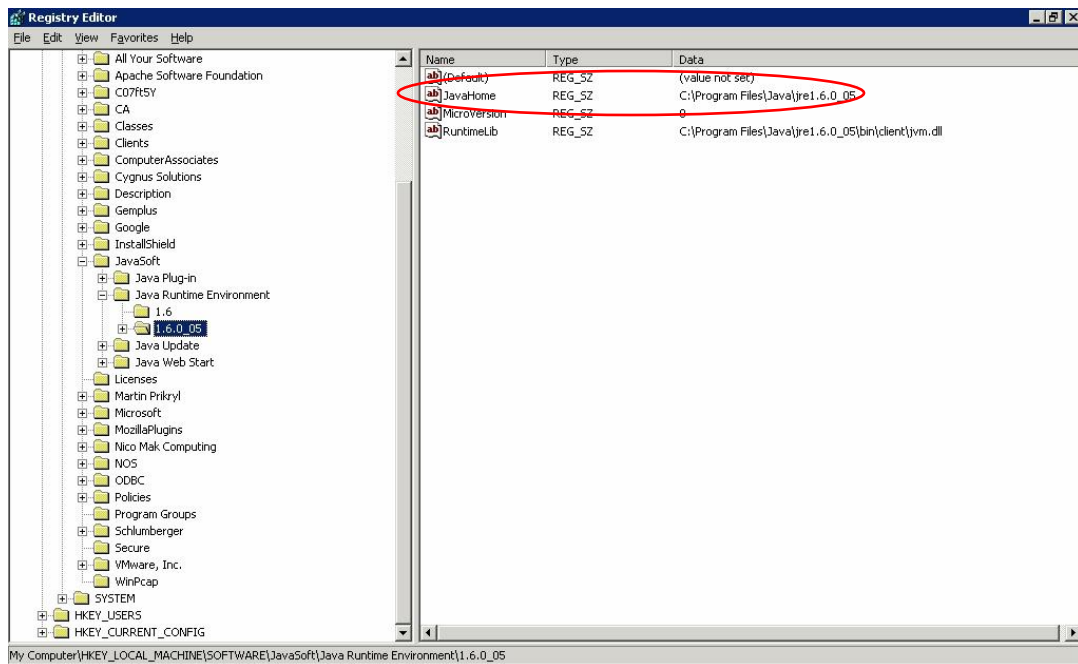
<http://www.java.com/en/download>

If you are unsure of the JRE location, then review following registry entry

HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Java Runtime Environment

This will show all JRE releases installed on the server. Select the latest one and drill into the JavaHome key. That is what you need to specify as "JAVA_HOME location".

For example, here you can see that JRE 1.6.0_05 is installed at under "C:\Program Files\Java\jre1.6.0_05"



8. Click **Next** to proceed.

Several CA EEM subcomponents will be installed.

9. Repeat these steps to install CA EEM on Node2.

Step 2: Define the CA EEM "ITPAM" Application Instance

Once CA EEM has been installed, the next step is to define the CA EEM "ITPAM" Application Instance. This needs to be defined on all CA EEM Servers. To create the ITPAM Application Instance do the following:

1. Change directory to CA IT PAM <cd2>:\EEM
2. Copy the ITPAM_eem.xml file from <cd2>:\EEM folder to your \iTechnology directory. The default location is:

C:\ProgramFiles\CA\SharedComponents\iTechnology

System Environment variable IGW_LOC can also be used to get to that location

```
Cd /d %IGW_LOC%
```

3. Change directory to the \iTechnology directory and execute the safex command.

```
Safex -h %COMPUTERNAME" -u EiamAdmin -p <your EiamAdmin Password> -f CA ITPAM_eem.xml
```

When the safex command is executed it will create the CA EEM "ITPAM" Application Instance as well as the CA ITPAMcert.p12 certificate in your \iTechnology directory.

```
C:\Program Files\CA\SharedComponents\it\technology>call safex.exe -h
-u EiamAdmin -p -f ITPAM_eem.xml
Setting back end to "1"
Setting locale to "en_us"
Detected EEM Server on host: [ ]
OK: Successfully Authenticated
OK: action[Attach] with ApplicationInstance label[]
OK: action[Register] performed on ApplicationInstance name[ITPAM] with label[ITPAM]
OK: action[Detach] from ApplicationInstance label[]
OK: action[Attach] with ApplicationInstance label[ITPAM]
OK: action[ReRegister] performed on ApplicationInstance name[ITPAM] with label[ITPAM]
OK: action[Skip] performed on object[Folder] name[/Policies]
OK: action[Skip] performed on object[Folder] name[/Users]
OK: action[Skip] performed on object[Folder] name[/UserGroups]
OK: action[Skip] performed on object[Folder] name[/System]
OK: action[Skip] performed on object[Folder] name[/Calendars]
OK: action[Add] performed on object[GlobalUser] name[/itpamuser]
OK: action[Add] performed on object[GlobalUser] name[/itpamadmin]
OK: action[Add] performed on object[UserGroup] name[/UserGroups/ITPAMUsers]
OK: action[Add] performed on object[UserGroup] name[/UserGroups/ITPAMAdmins]
OK: action[Modify] performed on object[UserGroup] name[/UserGroups/ITPAMAdmins]
OK: action[Add] performed on object[User] name[/itpamuser]
OK: action[Add] performed on object[User] name[/itpamadmin]
OK: action[Add] performed on object[Policy] name[/Domain Policy]
OK: action[Add] performed on object[Policy] name[/Environment Policy]
OK: action[Add] performed on object[Policy] name[/Itpam User Policy]
OK: Total objects Added[10]
OK: Total objects Modified[2]
OK: Total objects Removed[0]
OK: Total objects Skipped[5]
OK: Total objects Exported[0]
```

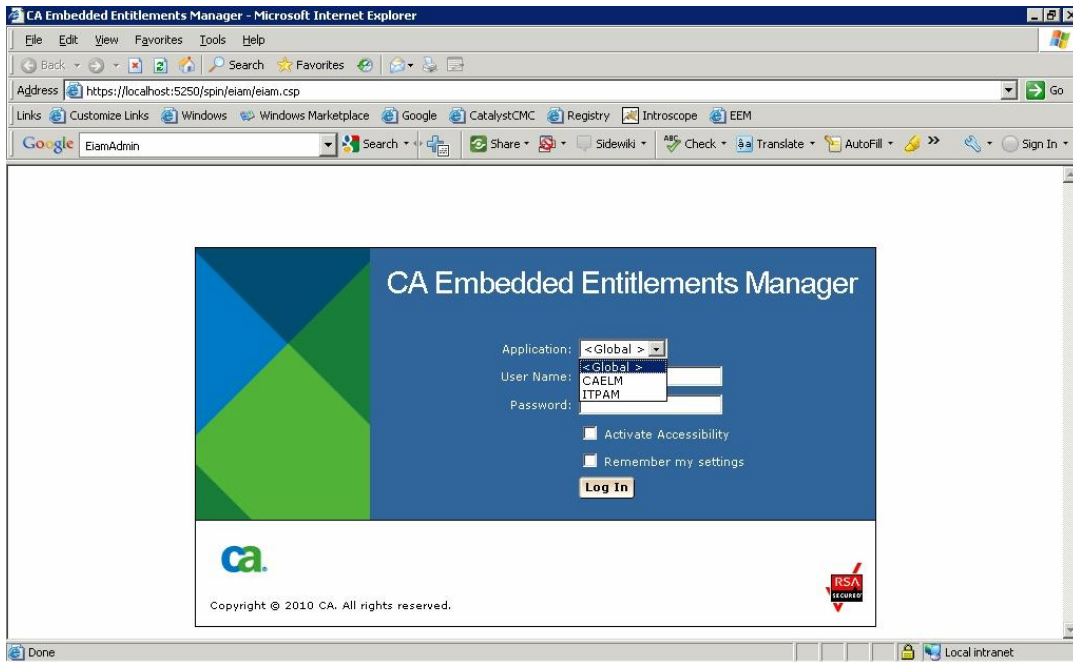
Note: The example above is from CA IT PAM r2.2 which includes additional data, such as policies, in the ITPAM_eem.xml file.. **CA IT PAM r3.0** also includes additional data, such as updated policies for the ConfigBrowser class.

Review the number of objects Added or Modified. If the ITPAM Application Instance was previously created then the numbers will vary. If the Total number of objects added is "0", this means that the safex command has been run before. If that is not the case, please check for any parsing errors.

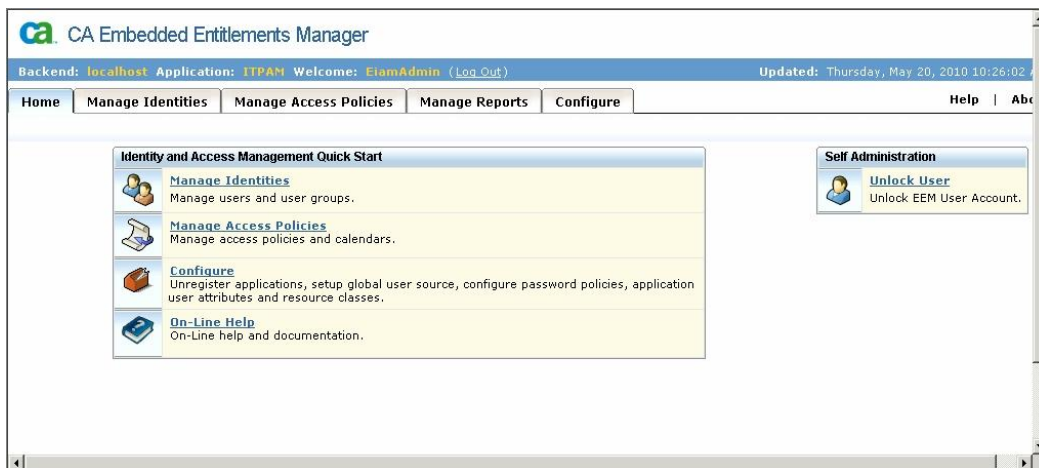
Verify the CA EEM ITPAM Application Instance

To confirm that the CA EEM ITPAM Application Instance has been added do the following:

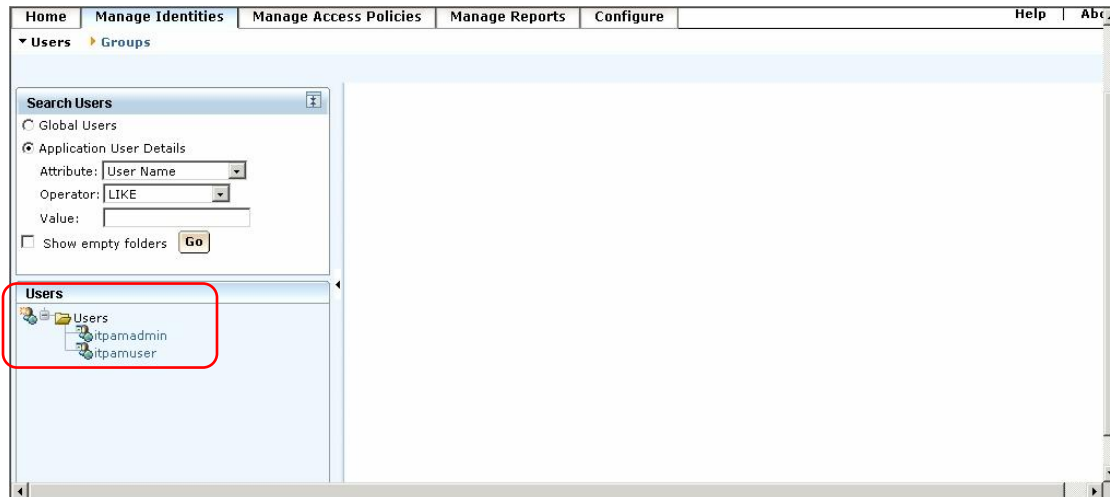
1. Launch the CA EEM UI
<https://localhost:5250/spin/eiam/eiam.csp>
2. Select "ITPAM" from Application drop down menu:



3. Enter the EiamAdmin password you specified during the CA EEM install and click Log In.
The CA EEM Home page will be displayed.



4. Select the Manage Identities Tab.
5. Select the Group tab
6. Verify "ITPAMAdmins" and "ITPAMUsers" application Groups are displayed



Step 3: Install CA EEM on Node2

Install CA EEM on Node 2 using the procedures listed earlier in Step 1. Repeat as needed for all additional nodes on which CA EEM is to be installed.

Step 4: Define the CA EEM “ITPAM” Application Instance for Node2

Define the CA EEM ITPAM Application Instance on Node 2 using the procedures listed earlier in Step 2. Repeat as needed for additional nodes on which CA EEM is installed.

Step 5: Configuring CA EEM to Use External Directory

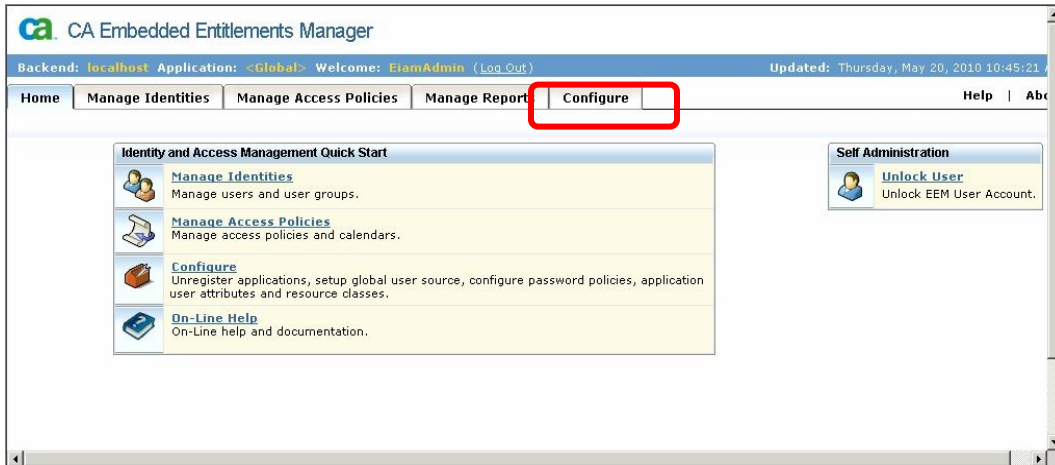
To enable CA IT PAM clients to use external usernames and passwords, you need to configure CA EEM to use external directories. To do this, do the following:

1. Launch the CA EEM UI

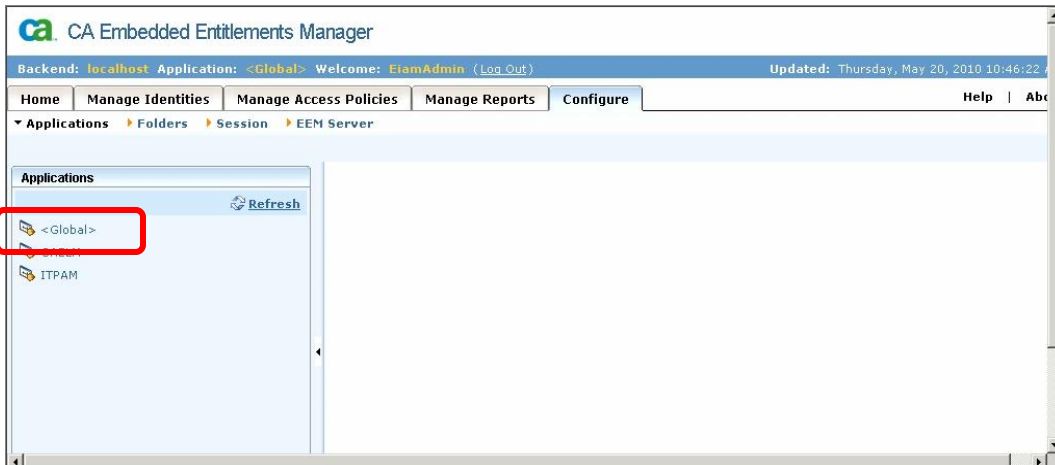
<https://localhost:5250/spin/eiam/eiam.csp>

The login dialog will display.

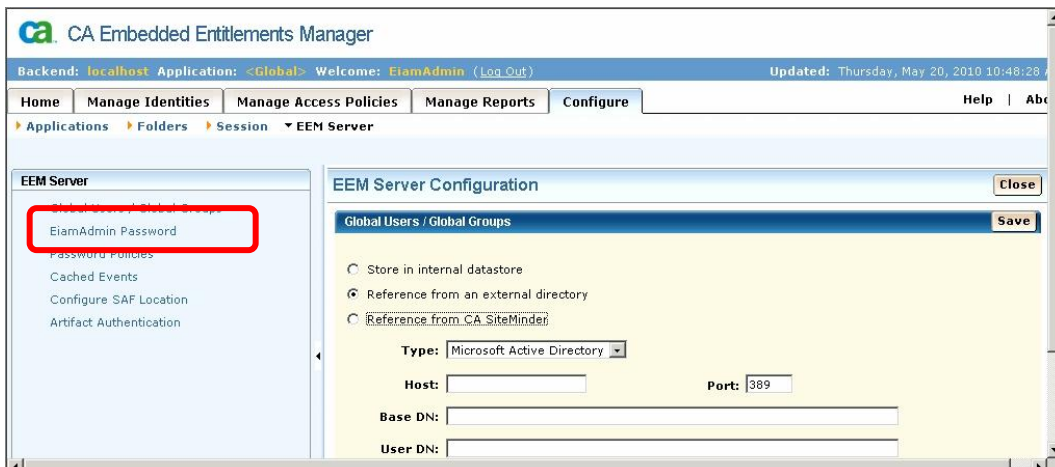
2. Select <Global> application, enter your EiamAdmin password and click **Login**.
3. Select the Configure Tab.



4. Select the EEM Server subtab:



5. Select Global Users / Global Groups:



6. Select the *Reference from an external directory* option and select the appropriate external directory from the *Type* drop down menu.

EEM Server

- Global Users / Global Groups
- EiamAdmin Password
- Password Policies
- Cached Events
- Configure SAF Location
- Artifact Authentication

EEM Server Configuration [Close]

Global Users / Global Groups [Save]

☐ Store in internal datastore
☒ Reference from an external directory
☐ Reference from CA SiteMinder

Type: Microsoft Active Directory
Host:
Port: 389
Base DN:
User DN:
Password:
Confirm Password:
☐ Use Transport Layer Security (TLS) ☐ Include Unmapped Attributes
☐ Cache Global Users **Cache update time:** 1440 (minutes)
☐ Retrieve Exchange Groups as Global User Groups

For example, here it shows the “Microsoft Active Directory” is selected.

EM Server

- Global Users / Global Groups
- EiamAdmin Password
- Password Policies
- Cached Events
- Configure SAF Location
- Artifact Authentication

EEM Server Configuration [Close]

☐ Reference from CA SiteMinder

Type: Microsoft Active Directory
Host: LDAPServer.ca.com Port: 389
Base DN: OU=myunit,DC=ca,DC=com
User DN: CN=myuser,OU=myunit,DC=ca,DC=com
Password:
Confirm Password:
☐ Use Transport Layer Security (TLS) ☐ Include Unmapped Attributes
☐ Cache Global Users **Cache update time:** 1440 (minutes)
☐ Retrieve Exchange Groups as Global User Groups

Status:
✓ External directory bind succeeded.
✓ External directory data is loaded.
Refresh status (without saving the changes)

[Close]

7. Provide the necessary BaseDN and UserDN details which can be obtained from LDAP administrator.
8. Click **Save** to save changes
9. Review the Status and ensure that *External directory bind succeeded* is checked. If this is not the case then the BaseDN, UserDN or password you provided is not correct.
10. Repeat the configuration on all other CA EEM nodes using same configuration details on each of them.

Now that CA EEM has been installed on the necessary nodes, the next step is to configure it for failover.

Step 6: Establishing a Trust Relationship Between the CA EEM Servers

In order to support failover between CA EEM servers you need to establish a trusted relationship between them. If this is not done, the cluster Node Domain will reject the request with an “Invalid user or password” error. To do this:

1. Logon to the first CA EEM Node (“Node1”). In our example, this is “DAWYA01V1”.
2. Change to the \iTechnology directory. By default this is:

C:\Program Files\CA\SharedComponents\iTechnology

For example:

CD /D %IGW_LOC%

3. Take a backup of the iControl.conf file

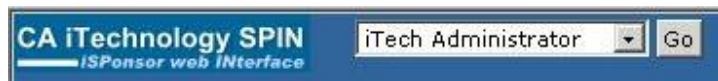
Copy iControl.conf iControl.conf_org

4. Configure Node1 (DAWYA01V1) to trust the backend CA EEM node ("Node2" – or, in our example, "DAWYA01V5") by adding a trust through the EIAM Spin GUI. To do this:

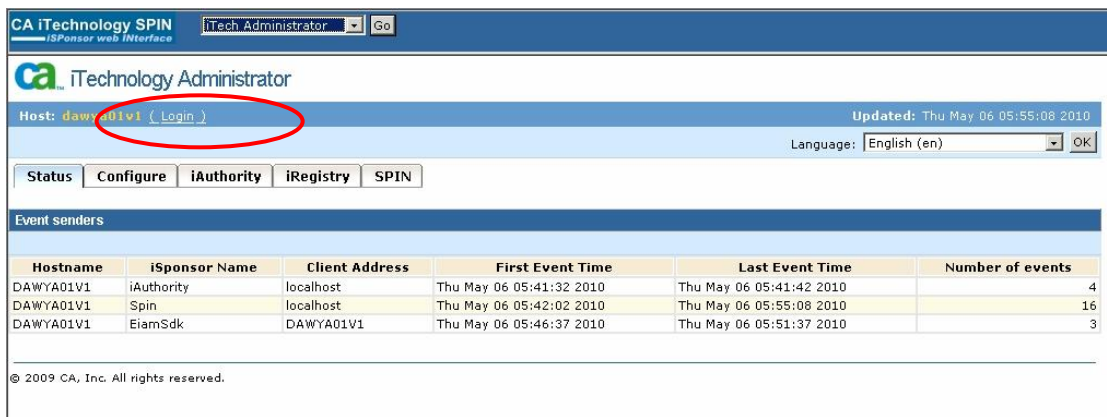
- a. Launch the Eiam Spin GUI by executing:

<https://localhost:5250/spin>

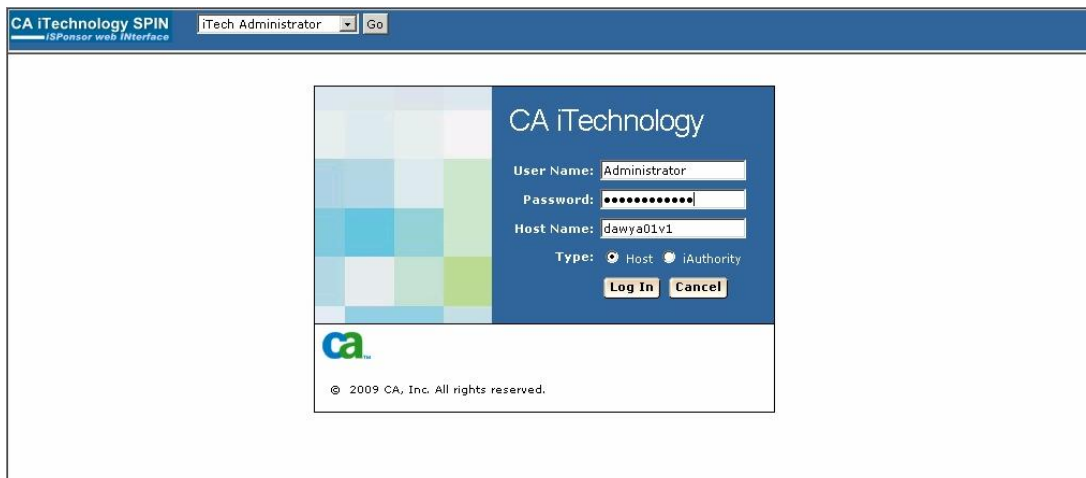
- b. Select iTech Administrator and click Go



- c. Login to Spin by clicking the Login link (next to your <hostname> (Login)):



- d. Provide your Windows credentials.



The credentials you provide must be valid to access the other CA EEM Servers for which the trust needs to be set up.

Tip! Ensure that the Host button is selected – not iAuthority!

If you do not have Windows credentials with administrative rights, you can login as iAuthority using with username EiamAdmin and the password you specified during the CA EEM install. In this case ensure that the iAuthority button is selected and not Host. This will also let you define Trusts and TrustedRoots.

Note: See Chapter 4: “Gotchas” for recommendations if you are have trouble logging in.

- e. Click the Configure tab and add the CA EEM Servers to be trusted under the “Trust Another iAuthority” field:

The screenshot shows the CA iTechnology SPIN iSPonsor web interface. At the top, there is a header bar with the title "CA iTechnology SPIN" and a sub-header "iSPonsor web interface". Below the header, there is a navigation bar with tabs: "Status", "Configure", "iAuthority", "iRegistry", and "SPIN". The "Configure" tab is selected. Below the navigation bar, there is a section titled "iControl Configuration" with an "Edit" button. This section contains a list of configuration parameters: "Start Time: Thu May 06 05:41:20 2010", "Events Received: 32", "Event Plugin:", "Route Events: false", "Route Events Host:", "Events To Cache: 100", "Saf Directory:", "Saf Expiration: 72", "Max Events Per Second:", "Ignore Signature: false", and "Credential Life Time: 24". Below this section, there is a section titled "Trusted iAuthority Hosts". This section contains a table with two columns: "Host name" and "Remove". The table has one row with the value "localhost" in the "Host name" column and a button with an "X" in the "Remove" column. To the right of the table, there is a dialog box titled "Trust another iAuthority". This dialog box has a "Hostname:" label and a text input field. A red rectangle highlights the "Trust" button in the dialog box.

For example, for the Node1 (DAWYA01V1), enter details for Node2 (DAWYA01V5). For the CA EEM Server on Node2 (DAWYA01V5), enter the details for Node1 (DAWYA01V1).

- f. Click the **Trust** button.

In our example, Node1 (DAWYA01V1) will start trusting sessions from Node2 (DAWYA01V5).

5. Confirm that the trust has been correctly setup by going to the \iTechnology directory and using Notepad to open the iControl.conf file and locate the <TrustedKey host> value. For example:

```
<TrustedKey host="DAWYA01V5"
name="DAWYA01V5">MIGJAoGBAMtFRjrKZueAVv6TGXbcrJmCX+YbztIJBcOryzSxZE6KR09t
1sG30hYFCLhsHI3WIj0h4JFfMxaFInzBL+IMuoIfL5Xayz8JZssQfWiZ7ZFnao6RanJjMaInd
c+7ygp5hSNecesuohjLXPTnrXuOUzfQ0uQd15TcYMilnAMockhDAgMBAAE=</TrustedKey>
```

6. Logon to Node2 (DAWYA01V5)
7. Repeat steps 2 to 5 to configure Node2 (DAWYA01V5) to trust Node1 (DAWYA01V1) by adding a Trust for Node 1 through the EIAM Spin UI.
8. Repeat as needed for all other CA EEM BackEnd servers.

Step 7: Define TrustedRoots for CA EEM Servers

The next step is to define TrustedRoots for the CA EEM Servers. This is also done using the CA EEM Spin GUI, however, if you are unable to login to Spin, you can set this manually as well. For additional information on how to configure TrustedRoots manually, review “Manually Configure TrustedRoots for CA EEM Backend Servers” later in this guide.

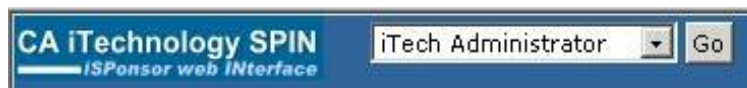
The following steps describe how to define TrustedRoots between CA EEM Server Node1 (DAWYA01V1) and CA EEM Server Node2 (DAWYA01V5)

1. Logon on Node1 (DAWYA01V1)
2. Map to the iTechnology directory on your Node2 (DAWYA01V5) drive.
By default this is C:\Program Files\CA\SharedComponents\iTechnology.
3. Login to Spin as before

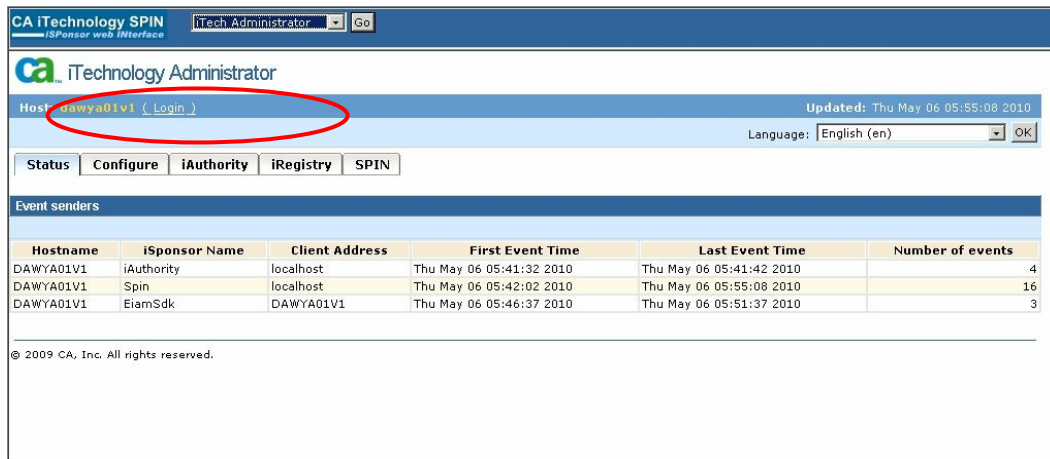
- a. Launch the Eiam Spin GUI by executing:

<https://localhost:5250/spin>

- b. Select iTech Administrator and click **Go**

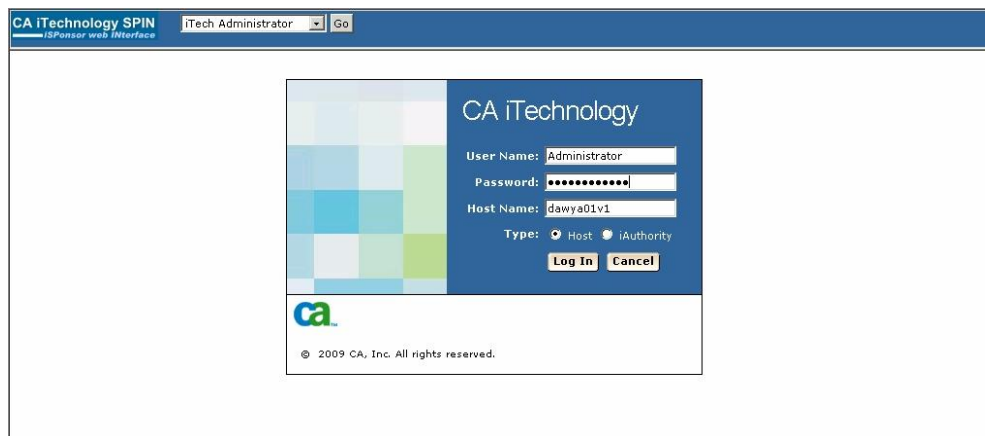


- c. Login to Spin by clicking the Login link (next to your <hostname> (Login)):



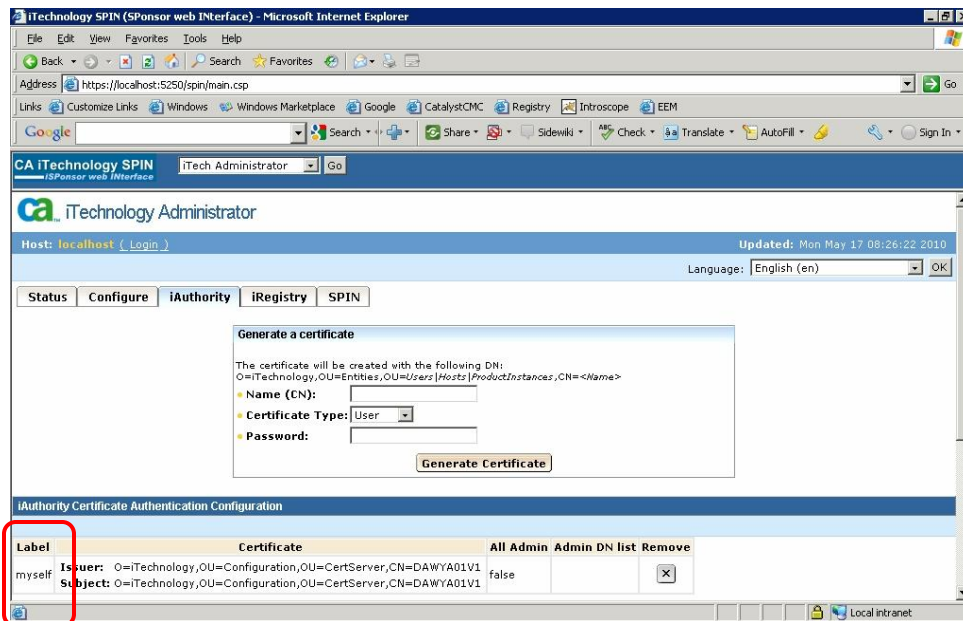
| Hostname | iSponsor Name | Client Address | First Event Time | Last Event Time | Number of events |
|-----------|---------------|----------------|--------------------------|--------------------------|------------------|
| DAWYA01V1 | iAuthority | localhost | Thu May 06 05:41:32 2010 | Thu May 06 05:41:42 2010 | 4 |
| DAWYA01V1 | Spin | localhost | Thu May 06 05:42:02 2010 | Thu May 06 05:55:08 2010 | 16 |
| DAWYA01V1 | EiamSdk | DAWYA01V1 | Thu May 06 05:46:37 2010 | Thu May 06 05:51:37 2010 | 3 |

d. Provide your Windows credentials.



If you are unable to login using valid Windows credentials then select the iAuthority option, enter “Eiamdmin” as User Name and provide the EiamAdmin password you specified during the CA EEM install.

- Click the iAuthority tab

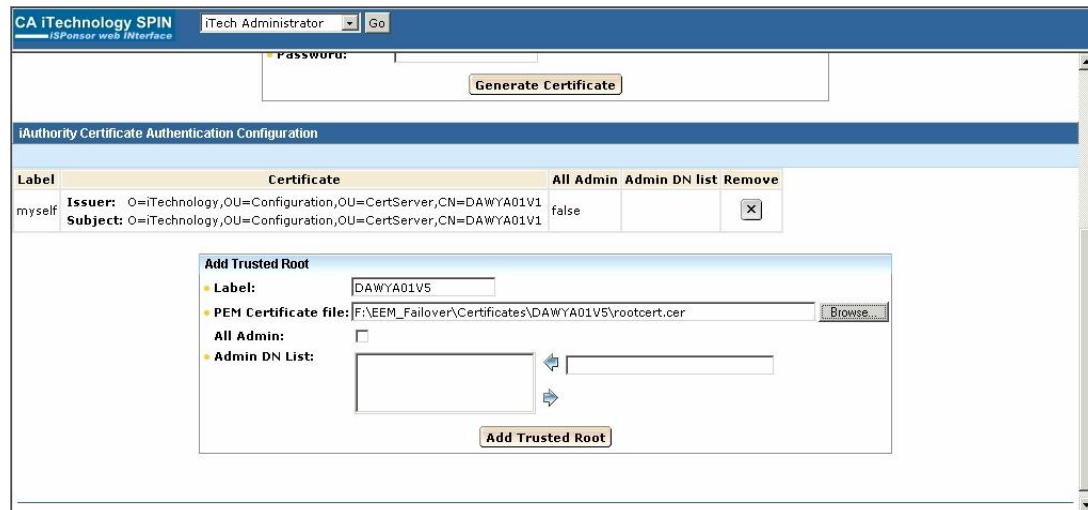


The “Label” column lists the CA EEM Servers for which trustedroot has been setup. In the example above, only the localhost (“myself”) is displayed which means that trustedroot for Node2 (dawya01v5) is not setup.

- Verify that the trustedroot for CA EEM Server Node2 (DAWYA01V5) is not already defined.

If it is not defined, provide a *Label* and *PEM Certificate file* details.

For example:



The PEM Certificate File is the rootcer.cer file and the location specified must be from the Node2 mapped drive (<mapped drive>:\Program Files\CA\SharedComponents\iTechnology).

6. Click **Add Trusted Root**

The screenshot shows the 'CA iTechnology SPIN iSPonsor web Interface'. The top navigation bar includes 'iTech Administrator' and a 'Go' button. The main content area is divided into two sections. The first section, 'Generate a certificate', contains a form with fields for 'Name (CN)', 'Certificate Type' (set to 'User'), and 'Password', along with a 'Generate Certificate' button. The second section, 'Authority Certificate Authentication Configuration', contains a table with columns: 'Label', 'Certificate', 'All Admin', 'Admin DN list', and 'Remove'. The table has two rows: 'myself' and 'DAWYA01V5'. The 'DAWYA01V5' row is highlighted with a red box. Below the table is the 'Add Trusted Root' section with fields for 'Label' and 'PEM Certificate file:' and a 'Browse...' button.

| Label | Certificate | All Admin | Admin DN list | Remove |
|-----------|---|-----------|---------------|----------------------------------|
| myself | Issuer: O=iTechnology,OU=Configuration,OU=CertServer,CN=DAWYA01V1 Subject: O=iTechnology,OU=Configuration,OU=CertServer,CN=DAWYA01V1 | false | | <input type="button" value="X"/> |
| DAWYA01V5 | Issuer: O=iTechnology,OU=Configuration,OU=CertServer,CN=DAWYA01V5 Subject: O=iTechnology,OU=Configuration,OU=CertServer,CN=DAWYA01V5 | false | | <input type="button" value="X"/> |

In the example above you can see that the trustedroot for DAWYA01V5 has been added.

7. Stop / Restart iGateway service
8. Logon to Node2 (DAWYA01V5)
9. Add TrustedRoot details for Node1 (DAWYA01V1) by repeating steps 2-7 for Node1

Manually Configure TrustedRoots for CA EEM Backend Servers

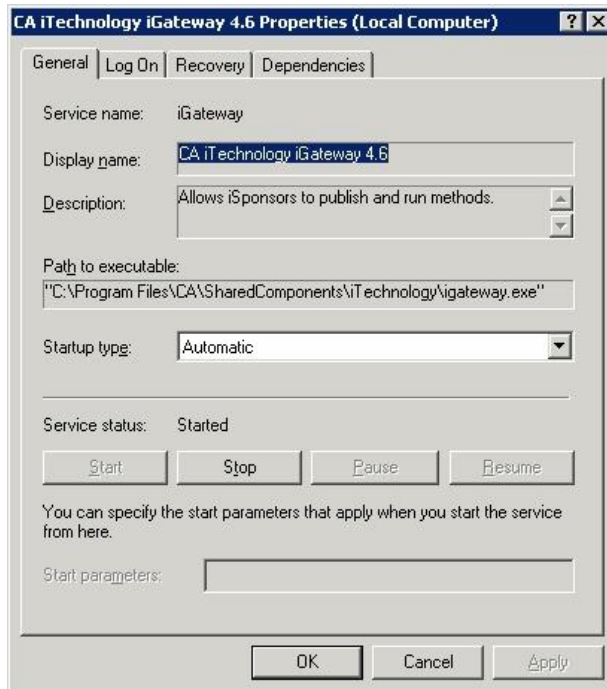
Use the procedures provided in this section only if you are unable to login to Spin. In some circumstances, Spin login to Host / iAuthority is rejected with invalid username or password.

In the following examples, Node1 is represented as "DAWYA01V1" and Node2 as "DAWYA01V5".

1. Logon to Node2 (DAWYA01V5) and map the \iTechnology drive on Node1 (DAWYA01V1):

```
Net use * \\dawya01v1\C$
```

2. Shutdown the iTechnology Gateway Service on both CA EEM nodes Node1 , Node2:



3. Change directory to the iTechnology directory on Node2(DAWYA01V5). For example:

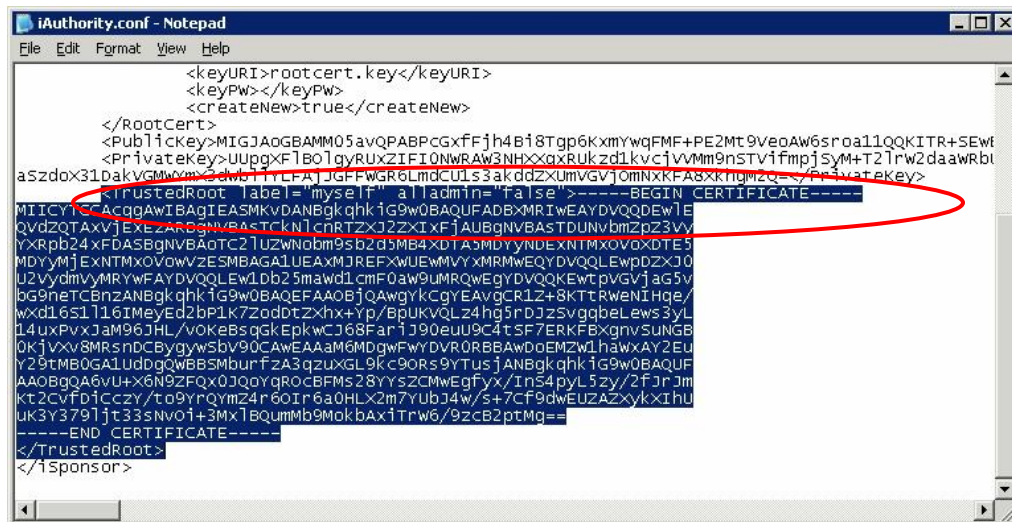
```
cd /d %IGW_LOC%
```

4. Use Notepad to open the iAuthority.conf file on Node1. This should be from the mapped drive. The default location is:

```
<mapped drive>:\Program Files\CA\SharedComponents\iTechnology
```

5. Locate the following <TrustedRoot label=" value.

For example:



In this example you can see that the value is:

```
<TrustedRoot label="myself" alladmin="false">
```

- Copy the text beginning with the TrustedRoot label up to and including </TrustedRoot> into your Node2(DAWYA01V5) iAuthority.conf file *local drive*. The default location is:

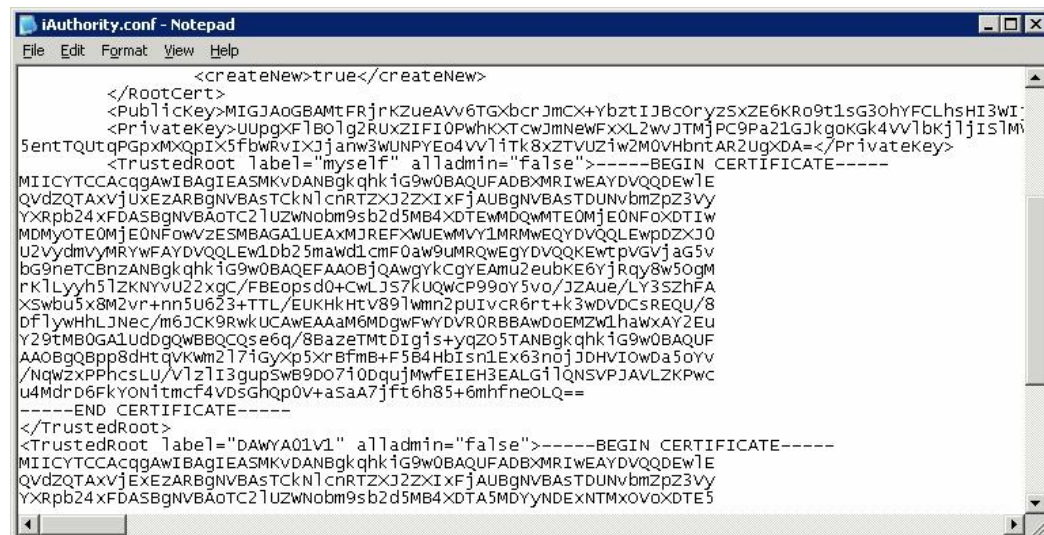
C:\Program Files\CA\SharedComponents\iTechnology

The lines to be included are:

```
<TrustedRoot label="myself" ...
...
-----END CERTIFICATE -----
</TrustedRoot>
```

- Change the value specified for TrustedRoot label in the copied lines from "myself" to "Node1"(DAWYA01V1).

In the following example you can see TrustedRoot tags for both nodes. Label "myself" refers to the local node which, in this case, is Node2. The label for the Backend CA EEM Node1 node is shown as "DAWYA01V1" and entry is copied from Node1 iAuthority.conf.



- Save the Node2(DAWYA01V5) iAuthority.conf file.
- Repeat steps 4-8 to update the Node1 iAuthority.conf file with the trustedroot from the Node2 iAuthority.conf file. In this case the "myself" label should be changed to "Node2" (DAWYA01V5)
- Start the iTechnology Gateway service on both nodes
- Stop CA Directory Services on **both** nodes. To do this execute the following:

```
Dxserver stop all
Ssld stop all
```



```

C:\>dxserver stop all
iTechPoz-DAWYA01C05-Router started
iTechPoz-DAWYA01C05-Router stopping
..
iTechPoz-DAWYA01C05-Router stopped
iTechPoz-DAWYA01C05 started
iTechPoz-DAWYA01C05 stopping
iTechPoz-DAWYA01C05 stopped

C:\>ssld stop all
Stopping iTechPoz-Server....
Stopped iTechPoz-Server
C:\>_

```

- Restart CA Directory Services on both nodes by executing the following:

```

Ssld start all
Dxserver start all

```

```

C:\>ssld start all
SSL 'iTechPoz-Server' configured with the following options
port 2447
certfiles C:\PROGRAM~1\CA\DIRECT~1\dxserver/config/ssld/personalities
ca C:\PROGRAM~1\CA\DIRECT~1\dxserver/config/ssld/iTechPoz-trusted.pem
debug 3
threads 0
protocol SSLv3
cipher ALL:!EXPORT40:!ADH
Starting iTechPoz-Server....
Started iTechPoz-Server

C:\>dxserver start all
iTechPoz-DAWYA01C05-Router stopped
iTechPoz-DAWYA01C05-Router starting
..
iTechPoz-DAWYA01C05-Router started
iTechPoz-DAWYA01C05 stopped
iTechPoz-DAWYA01C05 starting
..
iTechPoz-DAWYA01C05 started
C:\>_

```

Step 8: Use the Resource Kit to Configure CA EEM Data Store Replication

When multiple CA EEM Servers are installed it is a good idea to synchronize the CA EEM Data Store so that, when a new CA IT PAM application user is added, that user is replicated on the other CA EEM Server nodes. A Resource Kit is available to assist in this process. This kit can be downloaded from the CA IT PAM Best Practices section of the Implementation Best Practices page:

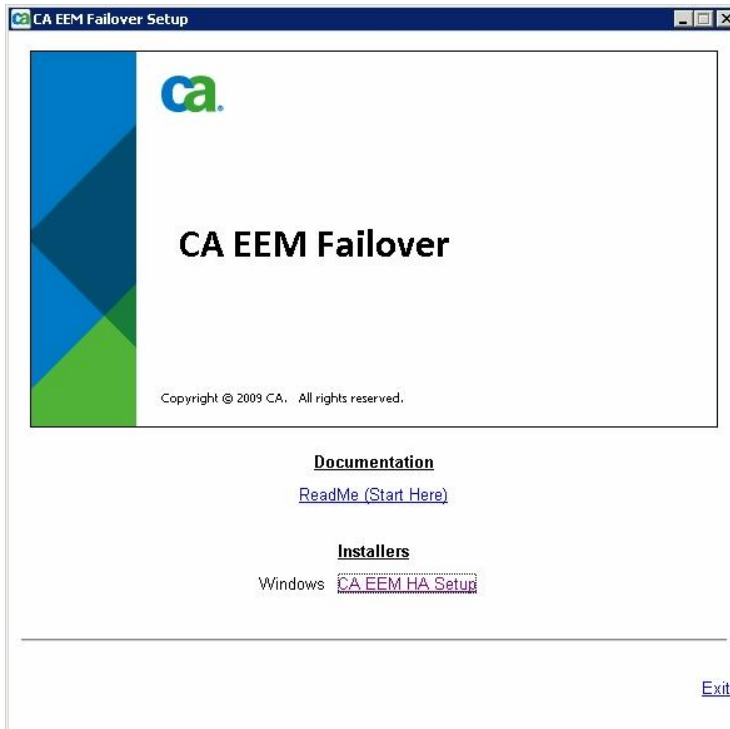
https://support.ca.com/phpdocs/0/common/impcd/r11/Catalyst/ITPAM_Frame_sc.htm

To setup Data Store Replication in a Microsoft Cluster environment using the Resource Kit, do the following:

- Download the CA EEM Data Store replication kit and copy it to a local drive:

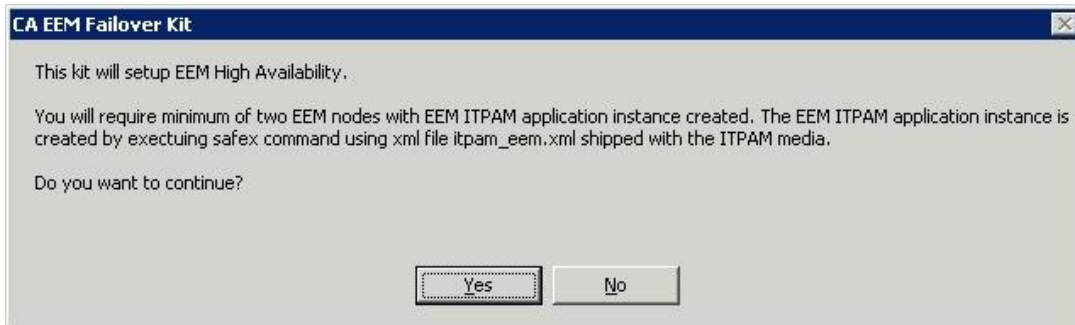
| Name | Size | Type |
|--------------|------|------------------|
| bin | | File Folder |
| Certificates | | File Folder |
| Docs | | File Folder |
| images | | File Folder |
| Logs | | File Folder |
| Nodes | | File Folder |
| setupEEM.hta | 7 KB | HTML Application |

2. Double-click setupEEM.hta



The Welcome dialog appears.

3. Click the CA EEM HA Setup link.



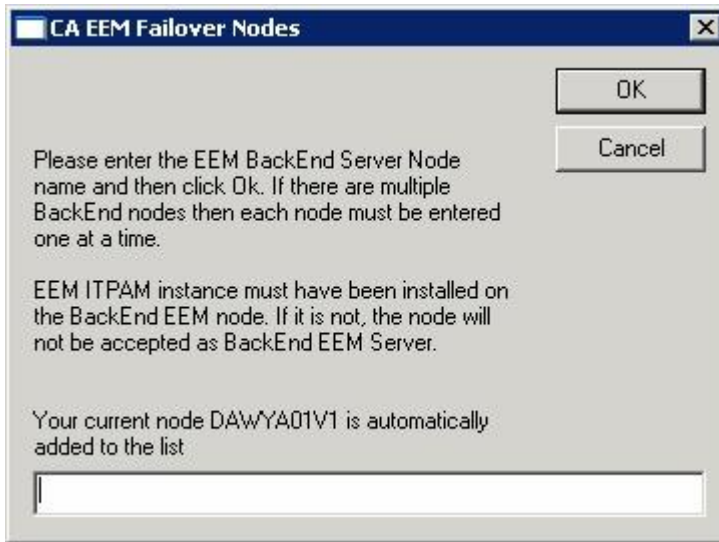
A message appears asking if you would like to continue with the configuration.

4. Click **Yes**.

The Resource Kit will verify that the CA EEM is installed and the CA EEM directory services are active.

Note: If CA EEM is not installed, an error message will be displayed. If the ITPAM Application Instance is not created or if CA EEM directory services are not active, the configuration will not continue.

If the CA IT PAM Application Instance exists and the required CA EEM directory services are active, you will see following screen



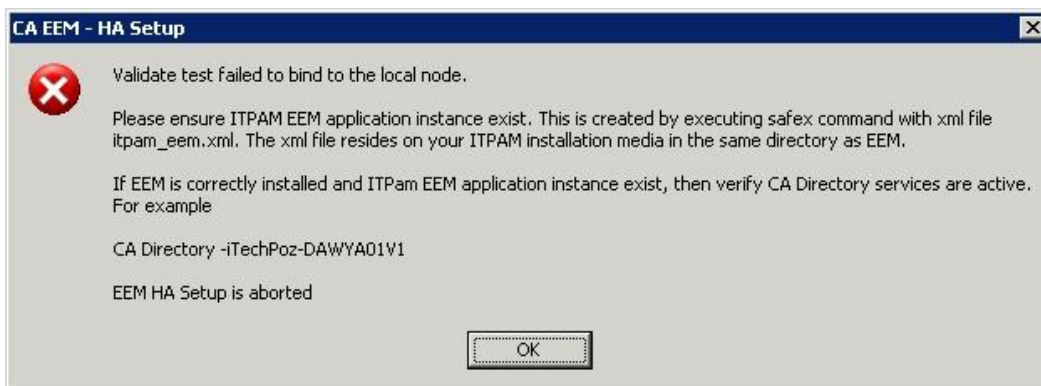
If CA EEM is not installed, you will see the following message



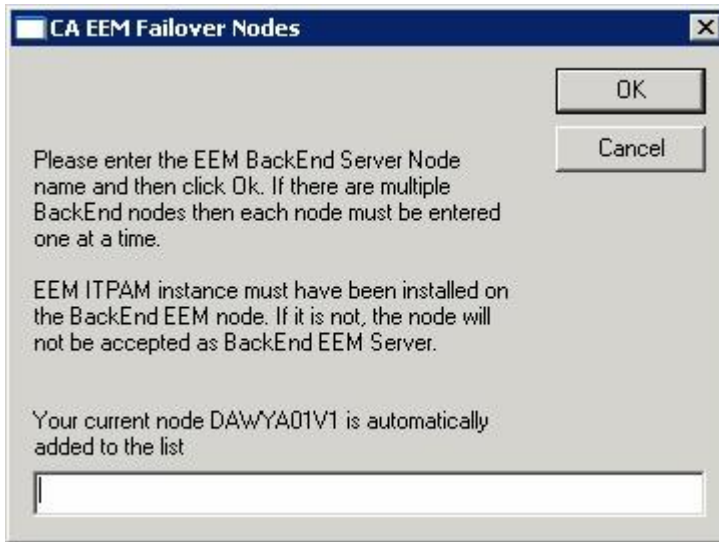
The setup will abort and the CA EEM ITPAM Application Instance will not be created.

If the CA EEM directory services are not active, the configuration will not continue.

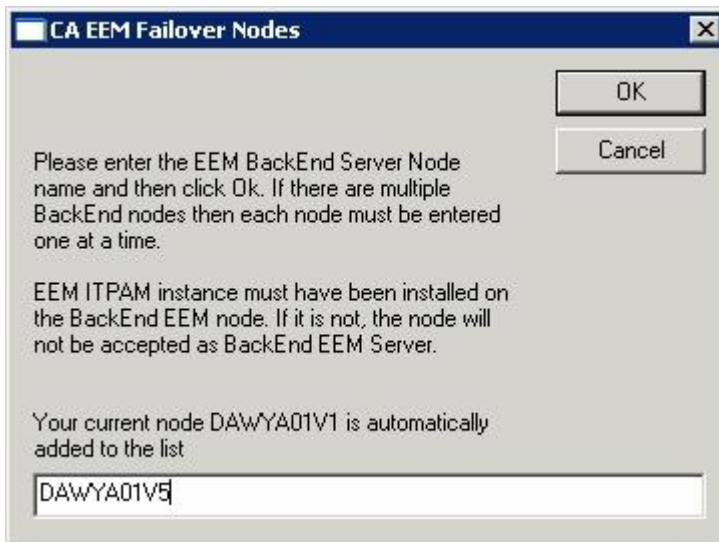
If CA EEM is installed but the CA IT PAM Application Instance is not created or if CA EEM services are not active then you will see the following messages and setup will be aborted:



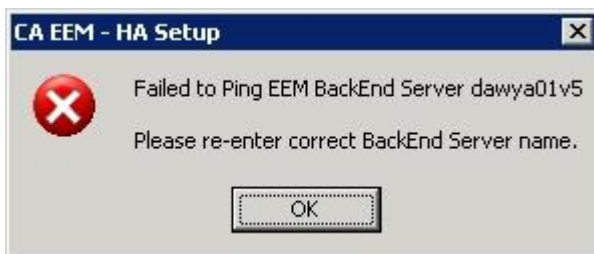
13. If the CA IT PAM Application Instance exists and the required CA EEM directory services are active you will be prompted to provide the name of the EEM BackEnd Server node. For example:



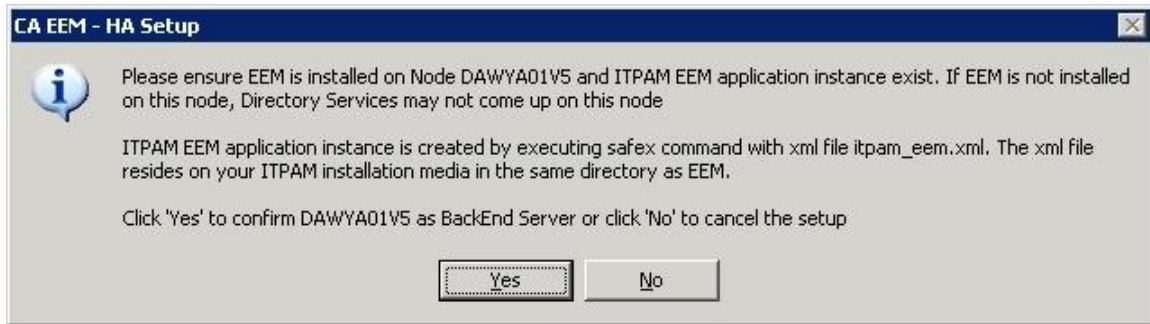
5. Enter the name of the CA EEM Node2 ("dawya01v5" in our example) and click **OK**



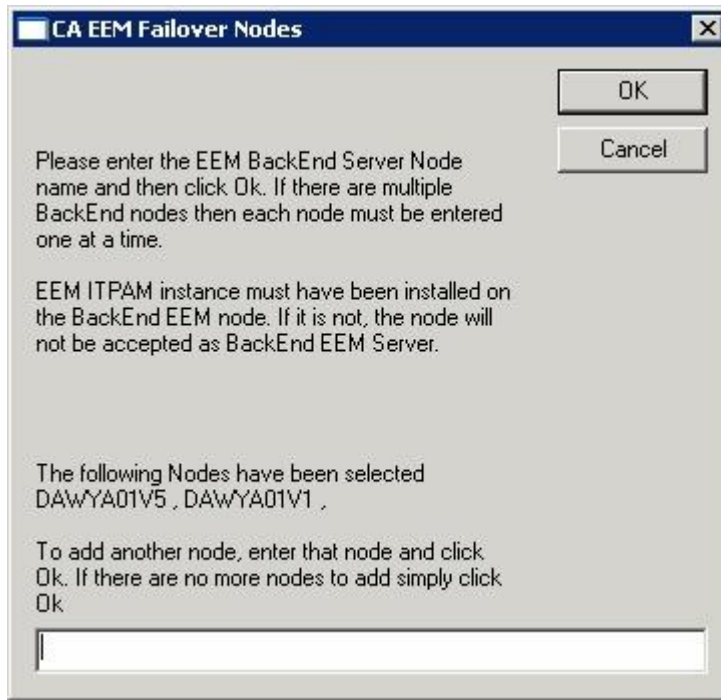
The Resource Kit will validate that node is pingable. If it is not, the following error will be generated:



If the CA EEM Server node is pingable, you will be prompted to confirm that the node should be added as the BackEnd server and should also participate in DataStore replication. For example:

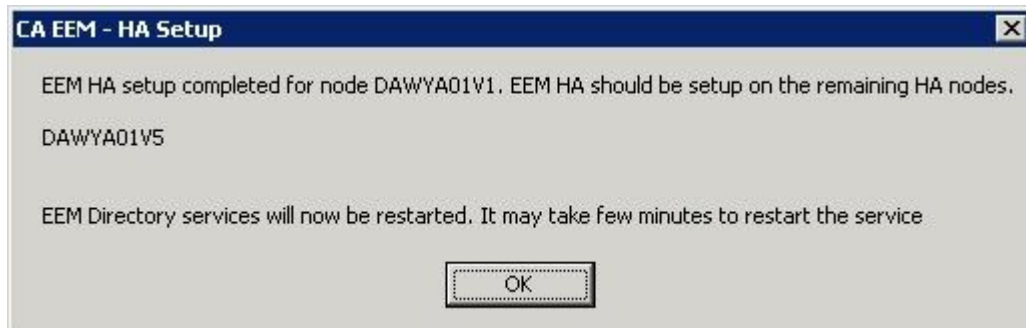


6. If you have already created the CA EEM ITPAM Application Instance on Node2, click **Yes** to add Node2 as the Backend Server.



If there are no more nodes to add, simply click **OK**.

7. The required updates will be made to setup DataStore replication and EEM failover.



If the configuration updates have been previously carried out, it will generate the following message and setup will be aborted.



8. Click **OK** to restart services



CA EEM Failover setup has now been successfully setup on Node 1. However, the failover or replication is not yet ready for use until the same configuration is carried out on Node2 as well.

9. Repeat the same for all other CA EEM Server nodes on that cluster.

Step 9: Install Load Balancer

Install the Apache Load Balancer. For detailed instruction review document *CA IT PAM Best Practices for Continuous and High Availability*.

Step 10: Install CA IT PAM

You are now ready to install the CA IT PAM Primary Domain Orchestrator. To do this:

1. Install and configure the Apache Load Balancer (see previous step)
2. Logon on to the server where CA IT PAM Primary Domain Orchestrator is to be installed.
3. Install CA IT PAM Primary Domain Orchestrator.
 - a. Ensure Load Balancer is configured for use.
 - b. Specify Node1 for the Load Balancer worker node. This definition must match the worker node specified in the Load Balancer configuration file worker.properties

Setup - CA IT PAM Domain 2.2

CA IT PAM Domain
Configuration Screen

☐ Configure Single Sign-on(SSO)

SSO Authentication Type: Header

SSO Authentication Parameter: sm-user

Type of server: New Server

☒ Configure Load Balancer

The load balancer worker node name is required by the Apache Load Balancer to uniquely identify this Orchestrator node in the cluster. User needs to add an entry for this name in the Apache workers configuration file before running this Orchestrator.

Load Balancer Worker Node: node1

Public Host Name: vmcluster

Public Host Port Number: 80

Public Host Secure Port: 443

☐ Support Secure Communication

< Back Next > Cancel

Load Balancer Worker Node details are defined in the Load Balancer workers.properties files:

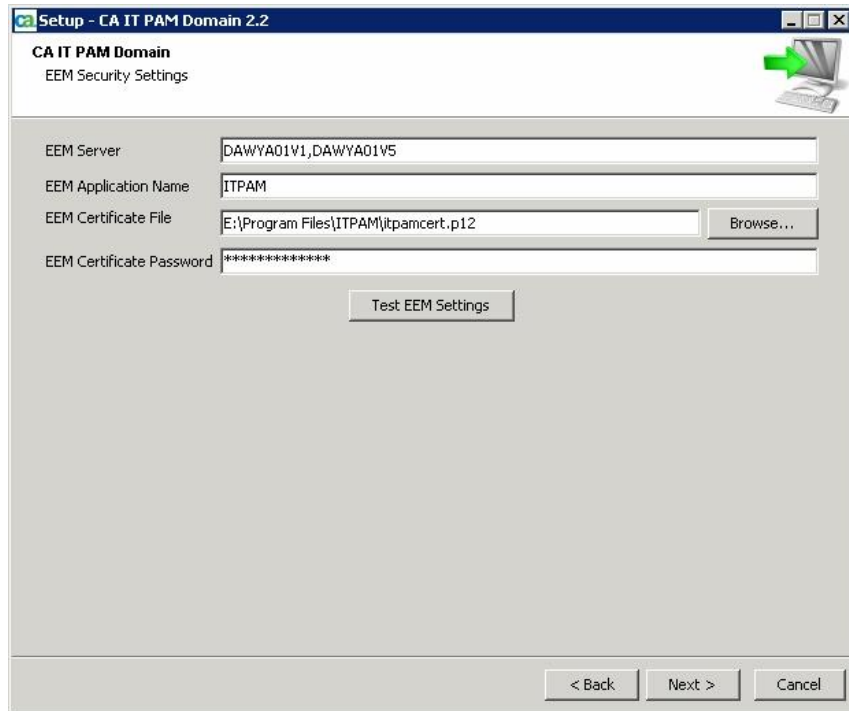
worker.node1.port=8009

worker.node1.host=<nodename_of_primary_Domain_Orchestrator>

worker.node1.type=ajp13

worker.node1.lbfactor=1

Specify the EEM Security Settings for the CA ITPAM Domain. For example:



The screenshot shows a Windows-style window titled "Setup - CA IT PAM Domain 2.2". Inside, the "EEM Security Settings" section contains four input fields: "EEM Server" with the value "DAWYA01V1,DAWYA01V5", "EEM Application Name" with "ITPAM", "EEM Certificate File" with "E:\Program Files\ITPAM\itpamcert.p12" and a "Browse..." button, and "EEM Certificate Password" with "*****". A "Test EEM Settings" button is located below these fields. At the bottom of the window are "< Back", "Next >", and "Cancel" buttons. A green arrow icon points towards the top right corner of the window.

In CA ITPAM r2.2 and above you can specify multiple CA EEM servers using a comma to separate each value (see example above). This feature is not available in earlier releases of CA ITPAM.

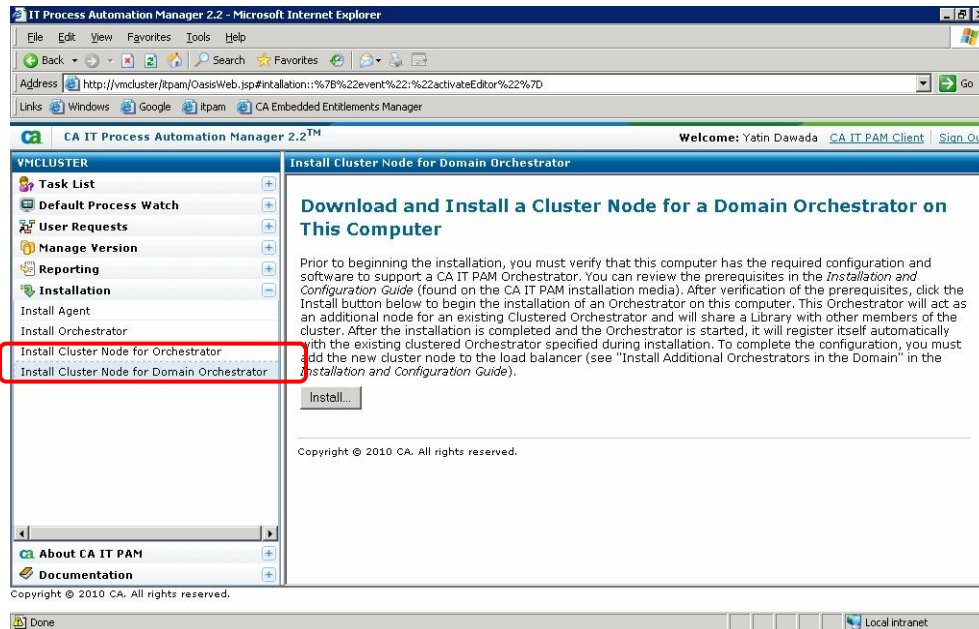
Note: If you are sharing CA EEM Servers with other applications which do not accept specification of multiple CA EEM servers as part of their CA EEM configuration, then you should consider installing CA EEM servers on a physical cluster such as Microsoft Cluster Services.

Important! If you specified multiple CA EEM nodes separated by a comma "Test EEM Settings" will only test the **first** CA EEM node in that list. If the subsequent CA EEM nodes in the list are not online or are not correctly configured, this will not be reflected by the "Test EEM Setting" results. To test these nodes, change the order of the CA EEM Servers listed and click **Test EEM Settings** again. For example, if you previously specified "Node1,Node2", change to "Node2,Node1" and click **Test EEM Settings**.

Step 11: Installing the Cluster Node Domain Orchestrator

To install the Domain Orchestrator on the Cluster node, do the following:

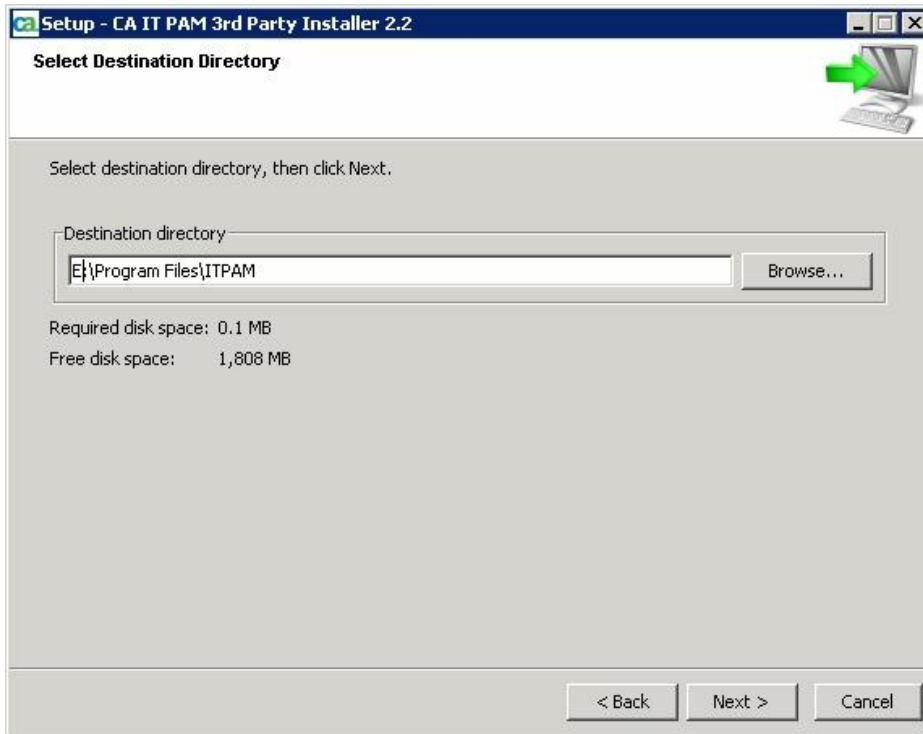
1. Logon to server where the CA IT PAM cluster node Domain Orchestrator will be installed.
2. Select “Install Cluster Node for Domain Orchestrator” from under the Installation heading in the left hand pane and click the **Install** button.



This will take you into the 3rd party installer setup.



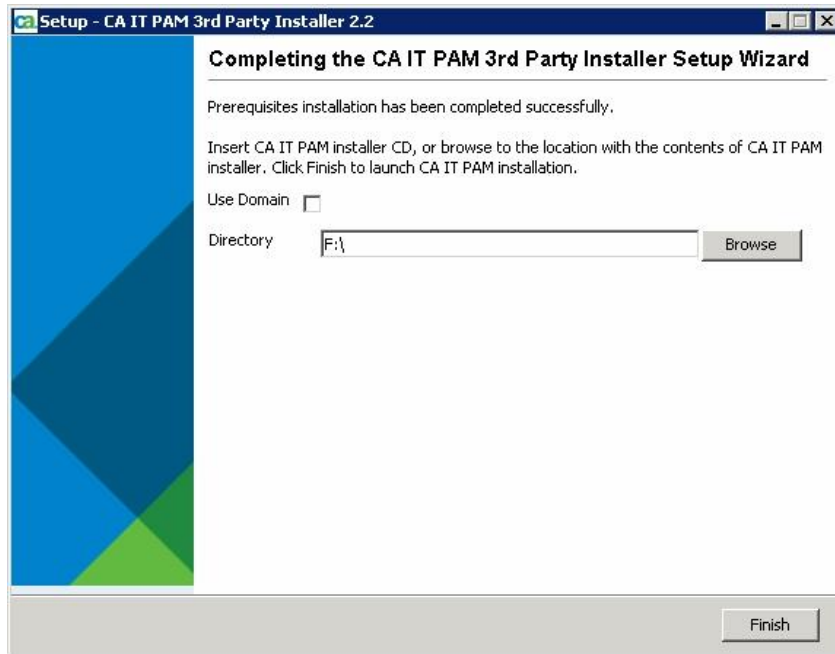
3. Click **Next** to proceed.
4. When prompted, specify Destination folder details and click **Next**:



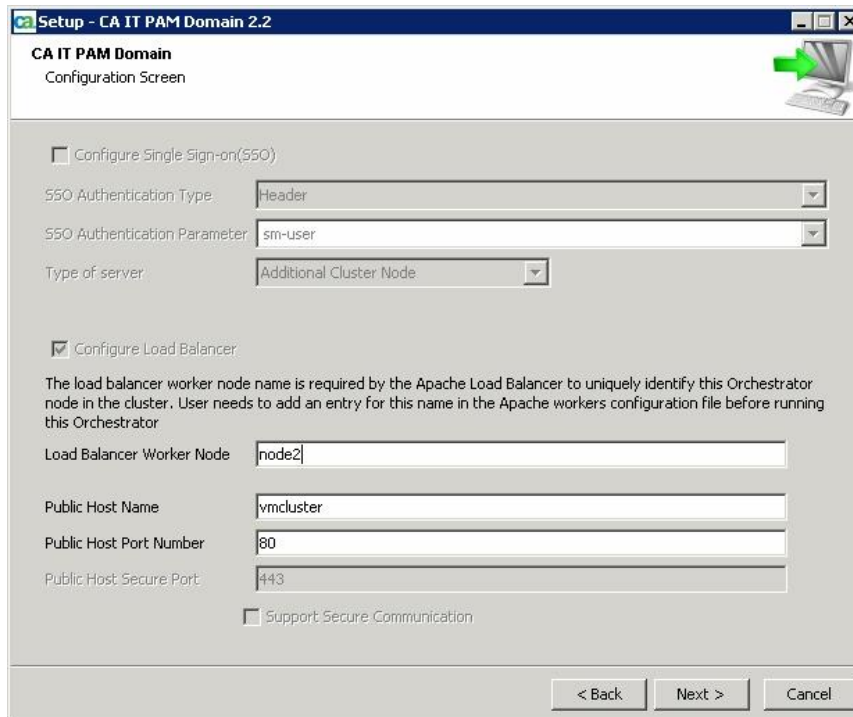
5. Check the 3rd Party prerequisites and click **Next**:



6. When the 3rd Party Install is completed, insert the CA IT PAM installation media or check the *Use Domain* checkbox to obtain the contents of the CA ITPAM installer from Primary Domain Orchestrator.



7. Click **Finish**.
8. Configure CA ITPAM to use the Load Balancer from the Setup dialog:



Note: The value specified for the Load Balance Worker Node must match your Load Balancer entries in the worker.properties file.

```
# Load-balancing behavior
worker.Primaryloadbalancer.type=lb
worker.Primaryloadbalancer.balance_workers=node2,node1
worker.Primaryloadbalancer.sticky_session=1
worker.Primaryloadbalancer.retries=1
```

Note: The value specified for Public Host Name is your Load Balancer Host Name.

Click **Next** to proceed. The Company details dialog appears.

9. Company Names details will be inherited from Primary Domain Orchestrator. Click **Next** to proceed.

The General Properties dialog appears.

Setup - CA IT PAM Domain 2.2

CA IT PAM Domain
General Properties

Server Host: DAWYA01PAM02

Display Name: VMCLUSTER

Server Port: 7001

Http Port: 8080

JNDI Port: 1099

RMI Port: 1098

SNMP Port: 162

Https Port: 8443

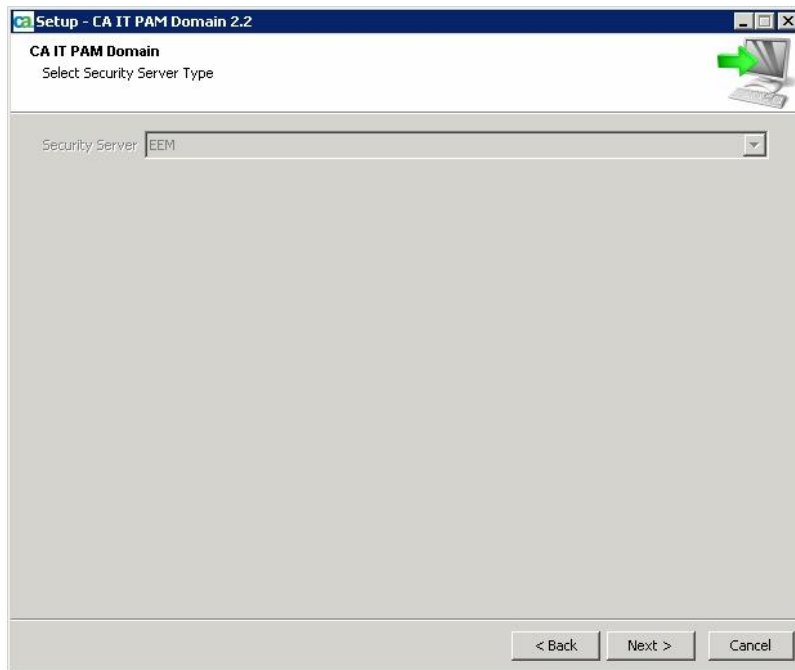
☐ Support Secure Communication

☒ Install as Windows Service

< Back Next > Cancel

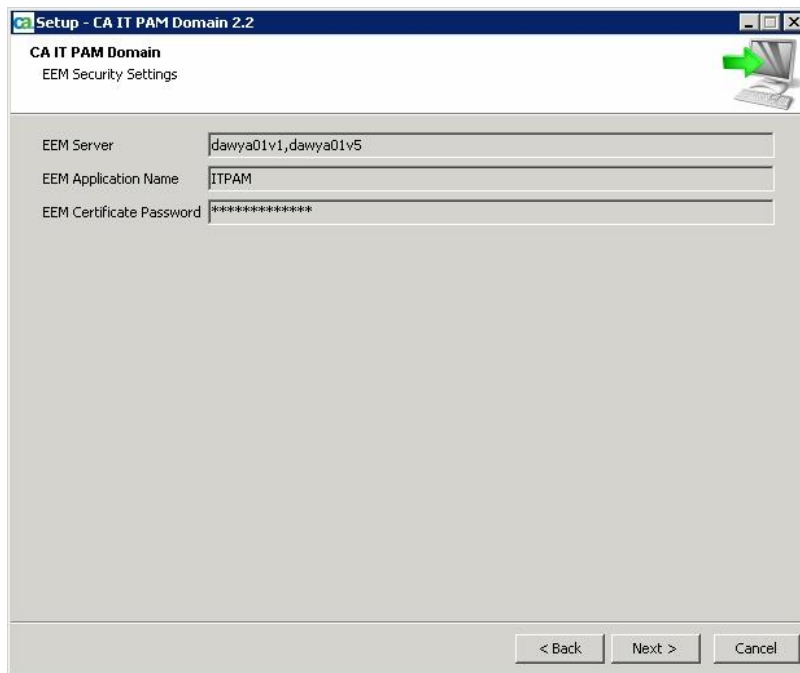
Provide the necessary details and click **Next**:

10. The Security Setting will be inherited from the Primary Domain.



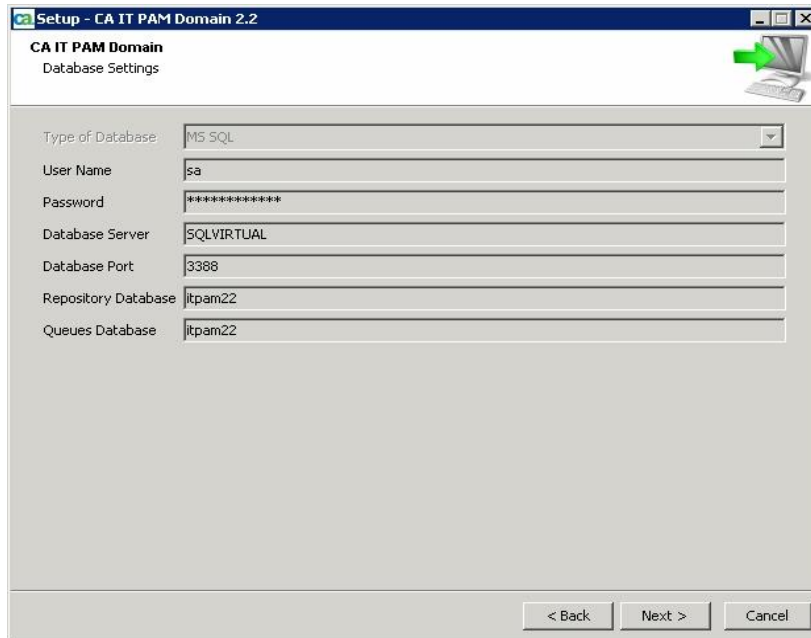
Click **Next** to proceed.

11. CA EEM details will be inherited from the Primary Domain.



Click **Next** to proceed.

12. Database and Reporting Database settings will be inherited from Primary Domain:



Setup - CA IT PAM Domain 2.2

CA IT PAM Domain
Database Settings

Type of Database: MS SQL

User Name: sa

Password: *****

Database Server: SQLVIRTUAL

Database Port: 3388

Repository Database: itpam22

Queues Database: itpam22

< Back Next > Cancel

Click **Next** to proceed.

13. Click **Finish**



Setup - CA IT PAM Domain 2.2

Completing the CA IT PAM Domain Setup Wizard

Setup has finished installing CA IT PAM Domain on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

Finish

14. Once the install is completed, verify that CA EEM works by logging onto the CA IT PAM Client.
15. Shutdown CA EEM Server Node1 and verify that you are able to still login to the CA IT PAM Client

Cluster Node Domain Orchestrator installation is complete. You should now be able to test your load balancer.

Logging on to the CA IT PAM Client

When the CA IT PAM client is launched, it must be addressed using the loadbalancer. In our example this is reached through the virtual node. For example:

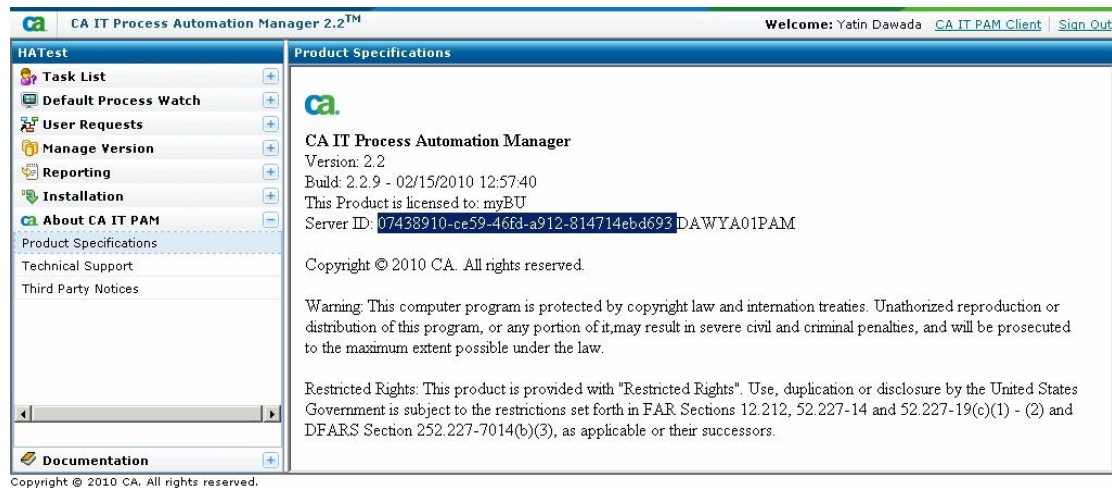
`http://<VMCLUSTER>/ITPAM`

where <VMCLUSTER> is the load balancer node name.

To identify the Domain Orchestrator to which the request has been routed by the load balancer do the following:

1. Login to the CA IT PAM Client.
2. Select "About CA IT PAM" in the left hand pane and compare the Server ID listed in the ServerID details against the value specified in the NodeConfiguration.properties file. This file resides in \Program Files\CA IT PAM\server\c2o\config.

For example, here you can see that the Hostname is also displayed since the copyright.jsp has been modified to display nodename for this test.



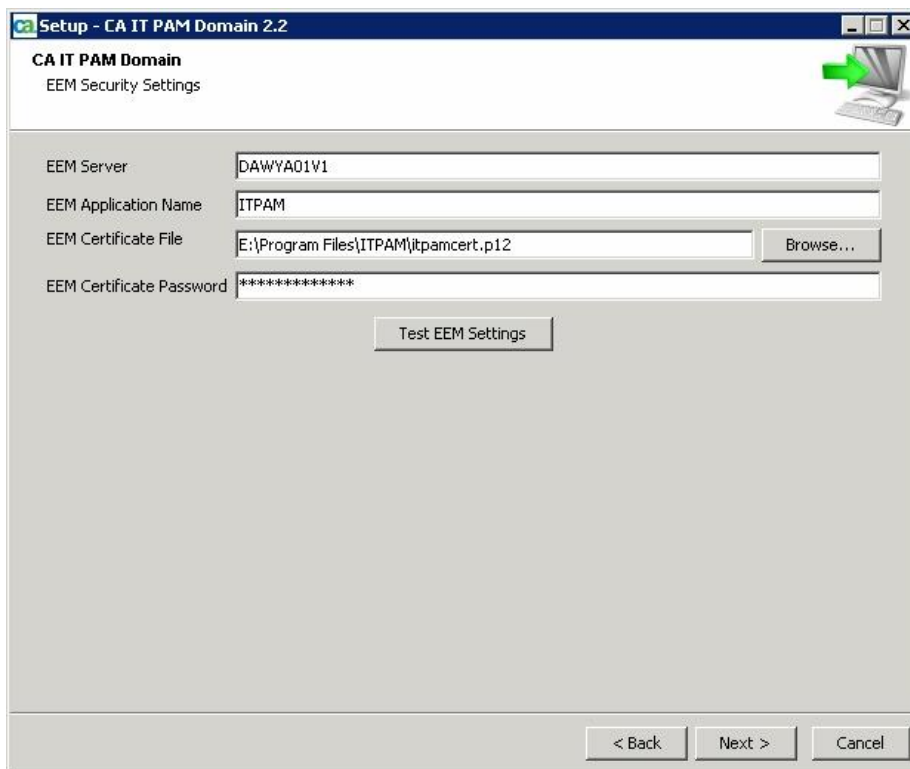
Last Updated: February 28, 2011

This will help you identify which Domain Orchestrator the loadbalancer has routed the request to. Consider the Server ID listed in the above example. Compare this to the entry in the following NodeConfigurations.properties file:



CA IT PAM EEM Settings

When you install the Primary CA IT PAM Domain (the first Domain that is installed is considered the "Primary Domain") you will be prompted to provide CA EEM details. For example:

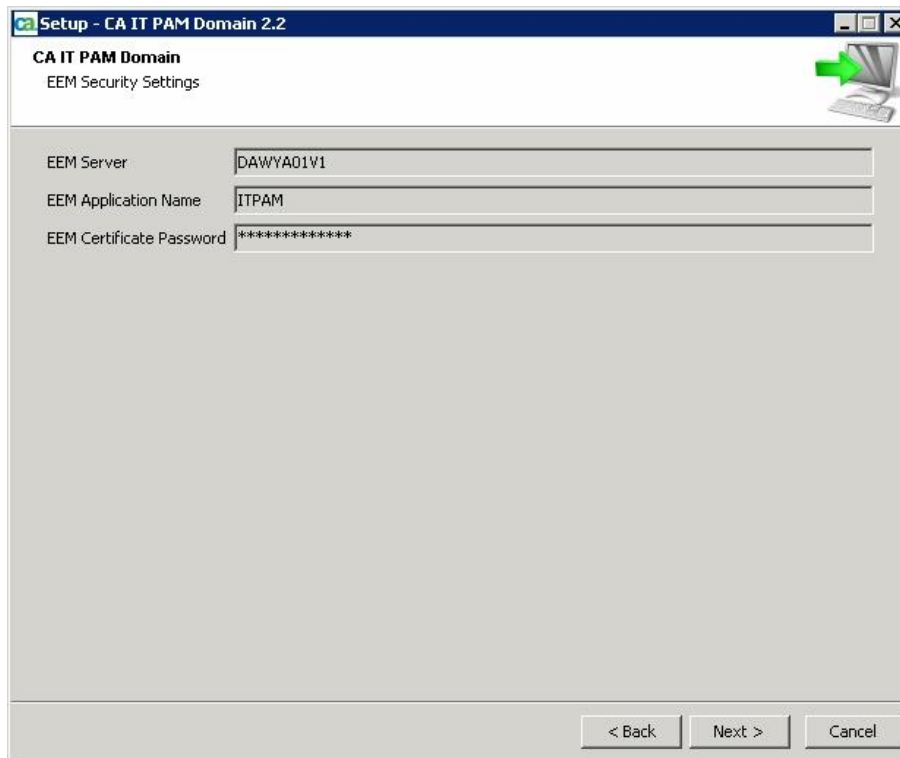


When the safex command is executed, it will create Itpamcert.p12 for the CA EEM ITPAM Application Instance. This will be created in the \iTechnology directory. The CA EEM Certificate Password is whatever is specified in the CA IT PAM_eex.xml file. The default is "itpamcertpass"

Here you can see the contents of itapm_eex.xml file:

```
<?xml version='1.0' encoding='UTF-8' standalone='no'?>
<Safex>
  <Attach/>
  <Register certfile="itpamcert.p12" password="itpamcertpass">
    <ApplicationInstance name="ITPAM" label="ITPAM" />
  </Register>
  <Detach/>
  <Attach label="ITPAM"/>
  <ReRegister>
    <ApplicationInstance name="ITPAM" label="ITPAM">
      <Brand>CA</Brand>
      <MajorVersion>2</MajorVersion>
      <MinorVersion>2</MinorVersion>
      <Translations>&lt;?xml version=&apos;1.0&apos; encoding=&apos;UTF-8&apos; standalone=&apos;no&apos;?&gt;
&lt;translations&gt;
  &lt;string&gt;
    &lt;key&gt;ITPAM&lt;/key&gt;
  &lt;/string&gt;
  &lt;string&gt;
    &lt;key&gt;CA&lt;/key&gt;
  &lt;/string&gt;
  &lt;string&gt;
    &lt;key&gt;Dataset&lt;/key&gt;
    &lt;en&gt;Dataset&lt;/en&gt;
  &lt;/string&gt;
  &lt;string&gt;
&lt;/translations&gt;
&lt;/ApplicationInstance>
&lt;/ReRegister>
&lt;/Safex>
```

For the secondary Domain install this will be inherited from Primary. For example:



The screenshot shows a Windows-style window titled "Setup - CA IT PAM Domain 2.2". Inside, the "CA IT PAM Domain" section is active, displaying "EEM Security Settings". There is a green arrow icon pointing to the right. Below the title bar, there are three input fields: "EEM Server" with the value "DAWYA01V1", "EEM Application Name" with the value "ITPAM", and "EEM Certificate Password" with a masked value "*****". At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

Chapter 3: Synchronize CA EEM Application Instances

This chapter provides information on how to backup Application Instance data so that it can be exported to another CA EEM server in the event the primary EEM server is down or to set up Disaster Recovery (DR).

When CA EEM failover is configured through the Resource Kit, Application Instance data is automatically replicated between multiple CA EEM Server Nodes. However, if CA EEM Failover was configured *after* updates were made to the CA IT PAM Application Instance then you need to synchronize the CA EEM Backend server. Note that DataStore replication only replicates *data that changes*. It will not synchronize any changes that occurred prior to CA EEM failover setup.

If you have not set up CA EEM failover and you plan to use another CA EEM Server for DR - or for any other reason - then you need to ensure that the CA IT PAM Application Instance is created on the DR Server and that the trustedroot has been set up on the DR server for the primary CA EEM Server.

The following Backup and Restore procedures document the steps to restore the CA EEM data but will not register / define any Application Instance. Thus, the CA EEM application must be registered prior to restoring the data. In addition, the backup procedure backs up the iPos for the server. This includes other Application Instances that may be registered on the primary CA EEM server.

Backup and Restore CA EEM Application Instances

Backup

To backup the CA EEM databases (Application Instances) do the following:

1. Download the toolkit to your EEM Server. For example: C:\EEM_Failover.
2. Change to the \Bin subdirectory. For example:

```
Cd EEM_Failover\Bin
```

3. Execute the supplied EEM_BackupRestore script using "Backup" as the first argument. For example:

```
EEM_BackupRestore Backup
```

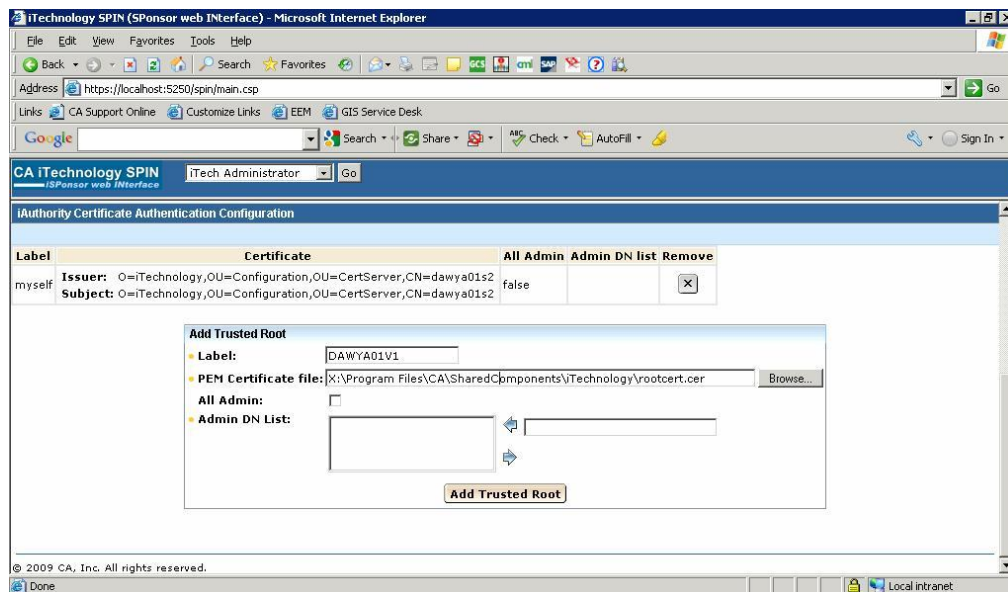
This script will temporarily stop CA EEM Directory Services, backup the CA EEM database and restart the Directory Services.

Restore

To restore the CA EEM databases on a different server - for example, to restore EEM Server Node1 to Node2 - do the following:

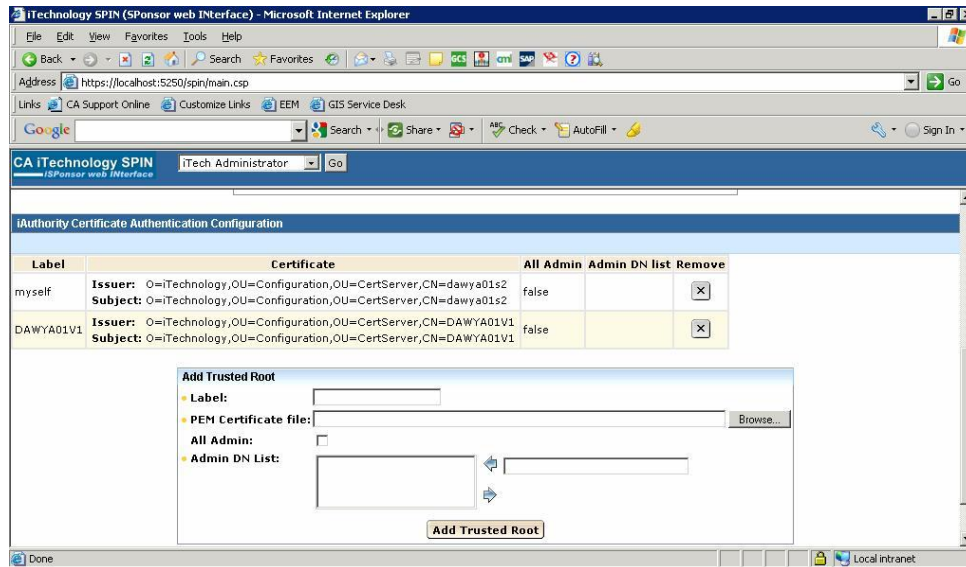
Note: If CA EEM Server Node1 is configured to use External Directory, Node2 should also be configured accordingly. Ensure External Directory is extracted and ready for use prior to restore. If CA EEM Server Node1 is configured to use External Directory and Node2 is not, then user policies that are restored may appear as orphaned users

1. Define Trust
2. Define TrustedRoots for Node1
 - a. Login EEM Node2 server
 - b. Map to Node1 iTechnology Drive
 - c. Login to EEM Spin using iAuthority
 - d. Define TrustedRoot for Node1 using Rootcer.cer from Mapped drive
 - e. Specify *Label* as “Node1”. In the following example, this is “DAWYA01V1”



In this example, TrustedRoot for CA EEM Server Node1 (DAWYA01V1) is added as it does not exist.

Here you can see the TrustedRoot for CA EEM Server Node1 (DAWYA01V1) has been defined to enable use of restored data from Node1 in Node2



For a detailed description on how to define TrustedRoots review Chapter 3 – Step 7.

3. Backup CA EEM from Node1. To do this execute the following command:

```
EEM_BackupRestore Backup
```

4. Verify CA EEM is installed on Node2
5. Verify that the CAEEM ITPAM Application Instance is created.

If it is not, create /register the CA EEM ITPAM Application Instance by executing the safex command. For additional information see “Step 2: Define the CA EEM ITPAM Application Instance” in Chapter 2.

6. Map a drive to where the \EEM_Failover directory resides on Node1. This is the directory to which the resource kit was downloaded and from where the eem_BackupRestore command was executed to backup the CA EEM Database.

7. Change to that directory. For example:

```
CD /D <Mapped Drive>:\EEM_Failover
```

8. Execute the following command:

```
EEM_BackupRestore Restore
```

The script executed by this command will stop Directory Services, restore the CA EEM database and restart the Directory Services and display restore statistics

9. Reconfigure CA IT PAM to use the CA EEM instance on to Node2.

See the “Updating the CA EEM Backend Server” section for additional information.

If you do not wish to use the script, then you can dump and load the CA EEM database using the following commands:

```
dxdumpdb -f <backup file lid filename> iTechPoz-%COMPUTERNAME%
dxloaddb -v -s -O iTechPoz-%COMPUTERNAME% < backup file lid filename >
```

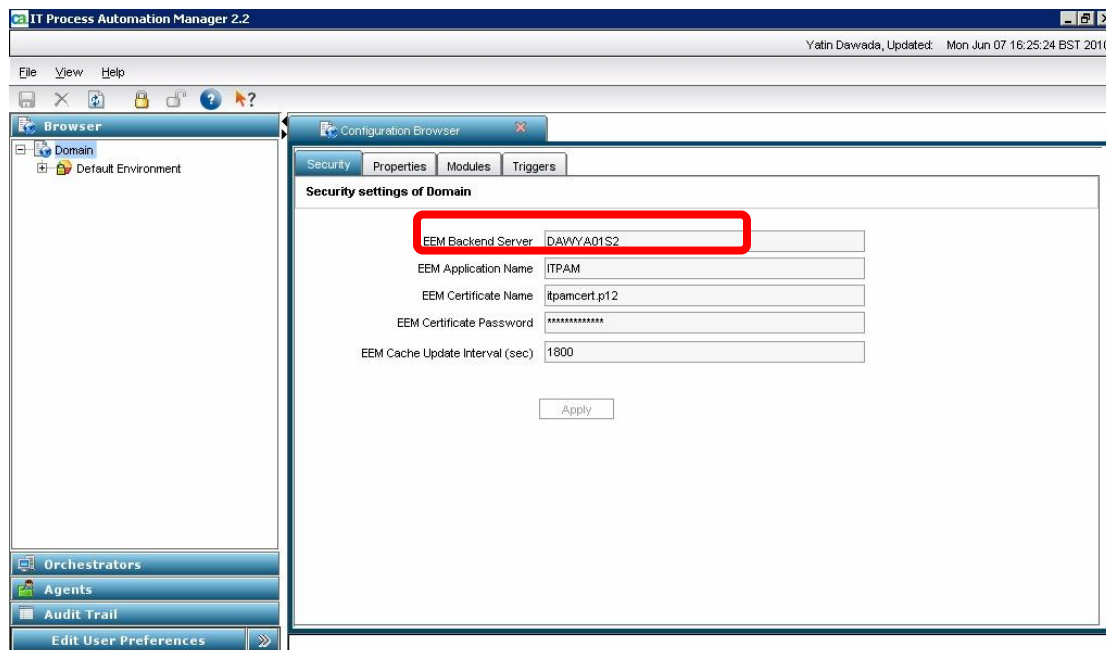
Updating the CA EEM Backend Server

If you have not configured CA EEM failover and were forced to change the CA IT PAM EEM server (for example, in the case of DR), then you will have to manually update the CA EEM Backend Server. This can be done in several ways:

- Through the CA IT PAM client, if you are able to login to it
- By reconfiguring the installation
- By updating the domain.xml. Note: This option should be last resort.

Update CA EEM Backend using CA IT PAM Client

If you are able to login to the CA IT PAM Client, then you update the CA EEM backend under the Security Settings for the Domain. For example:



Once the changes are saved, stop and re-start the CA IT PAM Orchestrator Window Service. When it restarts, it will use the new CA EEM server.

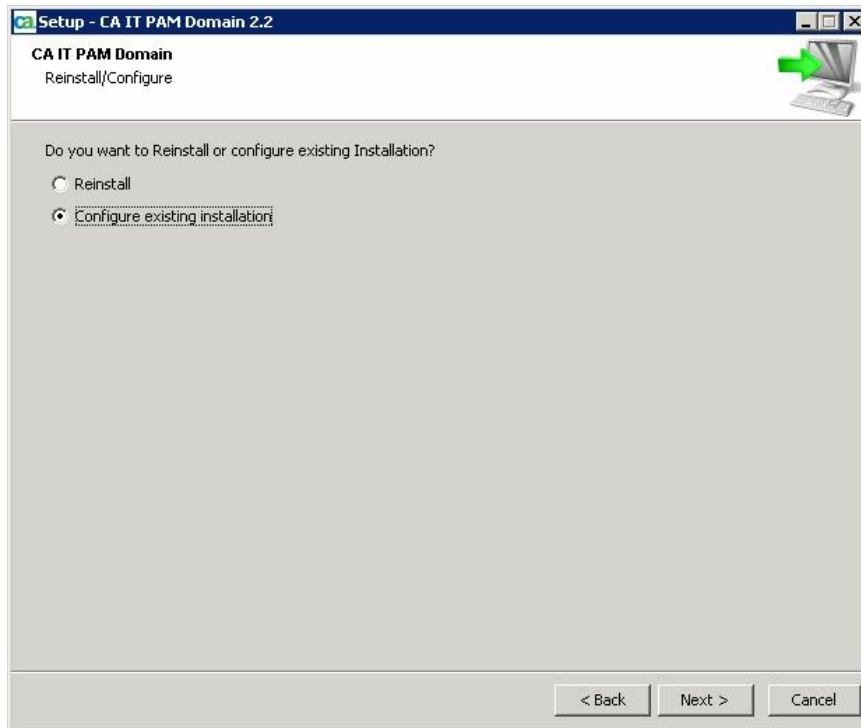
Reconfigure Existing Installation

If you are unable to login to the CA IT PAM client, then you can reconfigure the installation by doing the following:

1. Login to the primary domain installer server.
2. Stop the CA IT PAM Orchestrator service if it is running.
3. Execute the following command from the `$installationDir/server/c2o/.c2orepository/thirdParty` directory:

CA_ITPAM_Domain_windows.exe

4. Select *Configure Existing Installation* and click **Next**.



5. Modify the CA EEM server settings as required.

Update domain.xml

If you are unable to login to the CA IT PAM Client or run reconfigure, you can manually update the domain.xml file to make these change, however, this should only be considered as a last resort. . If you do decide to make changes to the domain.xml it is highly recommended that you first take a backup copy of the file so that it can be quickly restored if needed.

The domain.xml file is located in the following directory:

`\Program Files\ITPAM\server\c2o\.config\`

Using Notepad, open the file and locate the <SecurityProperties> “macroVal” value. Update this value to point to the new CA EEM server. Similarly, just below macroVal there should be a value tag. Update that tag as well to reflect the new CA EEM Server.

```

</C20Field>
<valueType
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="java:java.lang.String">ValueMap</valueType>
</C20Properties>
<SecurityProperties>
  <C20Field>
    <name>EEMBackendServer</name>
    <C20FieldDisplayInformation>
      <page>Security</page>
    </C20FieldDisplayInformation>
    <C20String>
      <macroVal>DAWYA01S2</macroVal>
      <value>DAWYA01S2</value>
      <valueType
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="java:java.lang.String">String</valueType>
      <C20StringConstraints>
        <C20MinLength>
          <MinLength>0</MinLength>
        </C20MinLength>
        <C20MaxLength>
          <MaxLength>2147483647</MaxLength>
        </C20MaxLength>
        <C20ReadOnly>
          <isReadOnly>false</isReadOnly>
        </C20ReadOnly>
        <canBeBlank>true</canBeBlank>
      </C20StringConstraints>
    </C20String>
  </C20Field>
  <C20Field>
    <name>EEMApplicationName</name>
    <C20FieldDisplayInformation>

```

Important! There are two sets of <SecurityProperties> and it is important that you update both of them. If the Domain Orchestrator was in Locked status, then it may revert back to the old settings.

Once the changes are saved, restart the CA IT PAM Orchestrator. Windows Service to pick the new Security changes.

Here you can see the CA IT PAM Orchestrator has connected to the new CA EEM Server but the login has failed as TrustedRoot was not defined.

```

0.0.0-8080-1] [com.ca.eiam.jpoz.PozFactory] runMethod - Leave : retVal[IclResult ir]
0.0.0-8080-1] [com.ca.eiam.SafeContext] setBackend - Leave
0.0.0-8080-1] [com.ca.eiam.SafeContext] authenticateWithCertificate - Enter : params[Certificate=E:\Program Files\ITPAM\server\c2o\c2oreposi
0.0.0-8080-1] [com.ca.eiam.jpoz.PozFactory] authorityLoginCert - Enter : params[Iclient icl, Authority=DAWYA01S2,CertFile=E:\Program Files\IT
0.0.0-8080-1] [com.ca.eiam.jpoz.PozFactory] authorityLoginCert - Leave : retVal=false
0.0.0-8080-1] [com.ca.eiam.SafeContext] authenticateWithCertificate - LoginFailed
0.0.0-8080-1] [com.ca.eiam.SafeCache] SafeCache - Enter
0.0.0-8080-1] [com.ca.eiam.SafeCache] SafeCache - Leave
0.0.0-8080-1] [com.ca.eiam.jpoz.PozFactory] PozFactory - Enter
0.0.0-8080-1] [com.ca.eiam.jpoz.PozFactory] PozFactory - Leave
0.0.0-8080-1] [com.ca.eiam.SafeContext] SafeContext - Enter
0.0.0-8080-1] [com.ca.eiam.SafeContext] SafeContext - m_cache=com.ca.eiam.SafeCache@15ff886, m_poz=com.ca.eiam.jpoz.PozFactory@1b52a38
0.0.0-8080-1] [com.ca.eiam.SafeContext] SafeContext - Exit
0.0.0-8080-1] [com.ca.eiam.SafeCache] setPersistentCacheFile - Enter : args[File=null]
0.0.0-8080-1] [com.ca.eiam.SafeCache] setPersistentCacheFile - Leave : args[File=null]
0.0.0-8080-1] [com.ca.eiam.SafeContext] setBackend - Enter : params[Backend=DAWYA01S2]
0.0.0-8080-1] [com.ca.eiam.jpoz.PozFactory] runMethod - Enter : params[Iclient icl,Host=DAWYA01S2,Sponsor=iAuthority,Method=GetPublicKey,List
0.0.0-8080-1] [com.ca.eiam.jpoz.PozFactory] checkForFailoverNumber: server returned with error code rc = 0
0.0.0-8080-1] [com.ca.eiam.jpoz.PozFactory] runMethod - Leave : retVal[IclResult ir]
0.0.0-8080-1] [com.ca.eiam.SafeContext] setBackend - Leave
0.0.0-8080-1] [com.ca.eiam.SafeContext] authenticateWithCertificate - Enter : params[Certificate=E:\Program Files\ITPAM\server\c2o\c2oreposi
0.0.0-8080-1] [com.ca.eiam.jpoz.PozFactory] authorityLoginCert - Enter : params[Iclient icl, Authority=DAWYA01S2,CertFile=E:\Program Files\IT
0.0.0-8080-1] [com.ca.eiam.jpoz.PozFactory] authorityLoginCert - Leave : retVal=false
0.0.0-8080-1] [com.ca.eiam.SafeContext] authenticateWithCertificate - LoginFailed
0.0.0-8080-1] [com.ca.eiam.SafeCache] stop - Enter
0.0.0-8080-1] [com.ca.eiam.SafeCache] stop - Bucket thread stopped
0.0.0-8080-1] [com.ca.eiam.SafeCache] stop - PollThread stopped
0.0.0-8080-1] [com.ca.eiam.SafeCache] writePersistentCache - Enter
0.0.0-8080-1] [com.ca.eiam.SafeCache] writePersistentCache - Leave
0.0.0-8080-1] [com.ca.eiam.SafeCache] trashEventQ - Enter
0.0.0-8080-1] [com.ca.eiam.SafeCache] trashEventQ - Leave
0.0.0-8080-1] [com.ca.eiam.SafeCache] stop - Event Thread stopped
0.0.0-8080-1] [com.ca.eiam.SafeCache] stop - HeartBeat thread stopped
0.0.0-8080-1] [com.ca.eiam.SafeCache] stop - Outstanding Event thread stopped
0.0.0-8080-1] [com.ca.eiam.SafeCache] stop - Stopped event Listeners
0.0.0-8080-1] [com.ca.eiam.SafeCache] stop - Leave

```

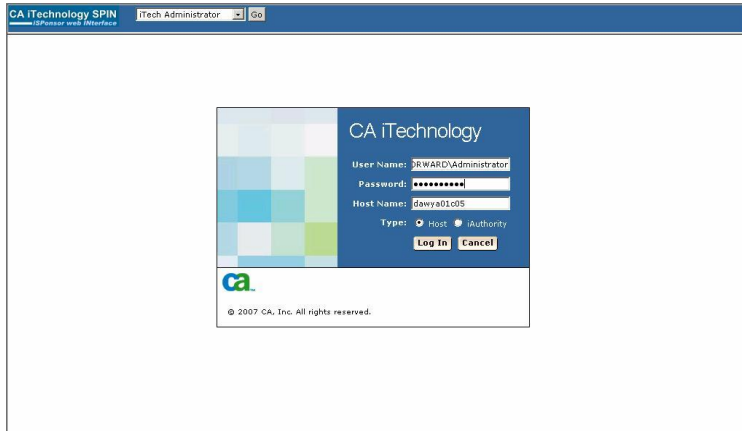
Once the TrustedRoot is defined the login will work.

Chapter 4: Gotchas

This chapter identifies several common problems that you may encounter during configuration.

Unable to Login to CA EEM Spin

To define the CA EEM Server trust, you have to login to the CA EEM GUI – iTechnology Page.



If you provide valid Domain credentials (with the “Host” radio button selected) but continue to receive a "Failed - Try again" error message it is likely the result of corrupted public and private keys stored in the "icontrol.conf" file. To remedy this, do the following:

1. Stop “CA iTechnology iGateway 4.x”
2. Change to the \iTechnology directory. By default this is:
`C:\Program Files\CA\SharedComponents\iTechnology`
3. Make a backup copy of the icontrol.conf file.
4. Open the icontrol.conf for editing and remove the "Public" and "Private" key tags.
5. Restart “CA iTechnology iGateway 4.x” service.

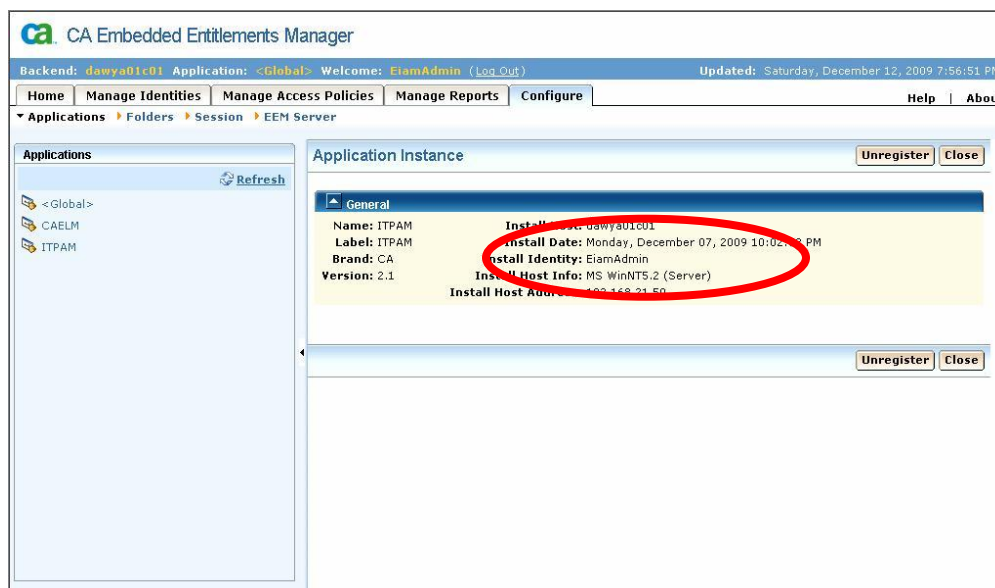
Here you can see the contents of iControl.cnf with the “PublicKey” and "PrivateKey" tags highlighted:


```
<?xml version='1.0' encoding='UTF-8' standalone='no'?>
<iSponsor>
  <Name>iControl</Name>
  <ImageName>iControl</ImageName>
  <Version>4.5.0.7</Version>
  <DispatchEP>iDispatch</DispatchEP>
  <IStype>DSP</IStype>
  <Gated>>false</Gated>
  <PreLoad>>true</PreLoad>
  <RouteEvent>>false</RouteEvent>
  <RouteEventHost>localhost</RouteEventHost>
  <EventsToCache>100</EventsToCache>
  <EventUseHttps>true</EventUseHttps>
  <EventUsePersistentConnections>true</EventUsePersistentConnections>
  <EventUsePipeline>false</EventUsePipeline>
  <StoreEventHost max="10000">localhost</StoreEventHost>
  <RetrieveEventHost interval="60">localhost</RetrieveEventHost>
  <UID>59c78959-DAWYA01C024b1cf7f0-aa6fd8-1</UID>
  <PublicKey>MIGJAoGBALXHKZ09DK0Qa48xGQHCoDubarpg3y2yJDM5GopwMAC5XEmj5jch5oEixnwJk+DTK
  <PrivateKey>UUpqXF1B0kUxM09DfmpEIW18XU26UjAtRjdmUz1Eb0MuK3qnXjVhKF1PTy10WUJ9P0R1THpd
  <TrustedKey host="localhost" name="localhost">MIGJAoGBAMD0rtNhrGUKvWRtvthMuJkEMhKA9D
  <EventCPlugin name="epiPoz">epiPoz</EventCPlugin>
  <TrustedKey host="DAWYA01C01" name="DAWYA01C01">MIGJAoGBAKM2ACmWt2yXQX3oyt882TUHTK/3
  <TrustedKey host="DAWYA01C05" name="DAWYA01C05">MIGJAoGBAK/KbU1gYfW/ymte/iZKj9171bTF
</iSponsor>
```

Unable to Login to CA IT PAM Client

If you have correctly configured trusted servers and shared trusted roots but you are still unable to login to the CA IT PAM thin client with valid credentials this could be because the CA EEM ITPAM Application instance was created from different host. To verify the install host of the ITPAM Application Instance do the following:

1. Login to the CA EEM GUI
<https://localhost:5250/spin/eiam>
2. Select <Global> from the *Application Instance* drop down and specify "EiaAdmin" as userid and its password
3. Click the Configure tab and then select CA IT PAM. This will display the Install Host as shown below

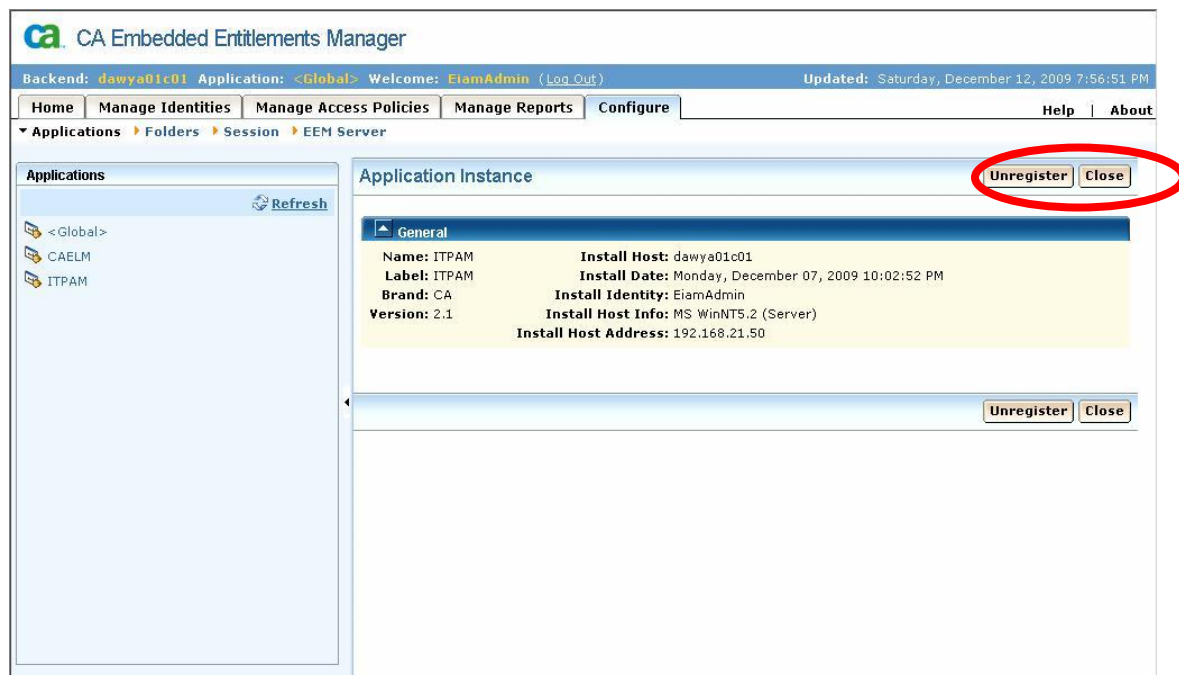


Removing the CA EEM ITPAM Application Instance

If the CA EEM ITPAM Application Instance is incorrectly configured, or if you wish to remove CA EEM, then you will need to delete the ITPAM Application Instance. This is also necessary if the CA EEM ITPAM Application Instance exists and you need to execute the safex command as the command will fail otherwise. In that case, you will have to delete the ITPAM Application Instance first and then execute the safex command to recreate it along with the certificate file.

To delete the CA EEM ITPAM Application Instance do the following:

1. Login to the CA EEM GUI by launching the following URL:
<https://localhost:5250/spin/eiam>
2. Select the <Global> Application Instance from the drop down list and specify “EiaAdmin” as userid and its password
3. Select the Configure tab and then select ITPAM from the list of Applications.
4. Click **Unregister**.



This will delete the CA EEM ITPAM Application Instance.

CA EEM Failover Detection

To determine if CA EEM failover has taken place, review the eiam.javasdk.log file. This file is located in the “Program Files\CA IT PAM\server\c2o\log\” directory.

Prior to failover, there is will be a timeout when a login is requested. For example:

```
at javax.security.auth.login.LoginContext$4.run(Unknown Source)
at java.security.AccessController.doPrivileged(Native Method)
at javax.security.auth.login.LoginContext.invokePriv(Unknown Source)
at javax.security.auth.login.LoginContext.login(Unknown Source)
at org.jboss.security.plugins.JaasSecurityManager.defaultLogin(JaasSecurityManager.java:572)
at org.jboss.security.plugins.JaasSecurityManager.authenticate(JaasSecurityManager.java:506)
at org.jboss.security.plugins.JaasSecurityManager.isValid(JaasSecurityManager.java:315)
at org.jboss.web.tomcat.security.JBossSecurityMgrRealm.authenticate(JBossSecurityMgrRealm.java:230)
at org.jboss.web.tomcat.security.FormAuthenticator.authenticate(FormAuthenticator.java:256)
at com.optinuity.c2o.server.C2OFormAuthenticator.authenticate(C2OFormAuthenticator.java:93)
at org.apache.catalina.authenticator.AuthenticatorBase.invoke(AuthenticatorBase.java:391)
at org.jboss.web.tomcat.security.JaccContextValve.invoke(JaccContextValve.java:59)
at org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:126)
at org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:105)
at org.jboss.web.tomcat.tc5.sso.ClusteredSingleSignon.invoke(ClusteredSingleSignon.java:366)
at org.apache.catalina.core.StandardEngineValve.invoke(StandardEngineValve.java:107)
at org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:148)
at org.apache.coyote.http11.Http11Protocol$Http11ConnectionHandler.service(Http11Protocol.java:856)
at org.apache.coyote.http11.Http11Protocol$Http11ConnectionHandler.doProcessConnection(Http11Protocol.java:744)
at org.apache.coyote.http11.Http11Protocol$Http11ConnectionHandler.process(Http11Protocol.java:527)
at org.apache.tomcat.util.net.PoolTcpEndpoint.processSocket(PoolTcpEndpoint.java:527)
at org.apache.tomcat.util.net.MasterSlaveWorkerThread.run(MasterSlaveWorkerThread.java:112)
Caused by: java.net.ConnectException: Connection timed out: connect
at java.net.PlainSocketImpl.socketConnect(Native Method)
at java.net.PlainSocketImpl.doConnect(Unknown Source)
at java.net.PlainSocketImpl.connectToAddress(Unknown Source)
at java.net.PlainSocketImpl.connect(Unknown Source)
at java.net.SocksSocketImpl.connect(Unknown Source)
at java.net.Socket.connect(Unknown Source)
at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
at sun.reflect.NativeMethodAccessorImpl.invoke(Unknown Source)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(Unknown Source)
at java.lang.reflect.Method.invoke(Unknown Source)
at org.apache.commons.httpclient.protocol.ReflectionSocketFactory.createSocket(ReflectionSocketFactory.java:139)
at org.apache.commons.httpclient.protocol.DefaultProtocolSocketFactory.createSocket(DefaultProtocolSocketFactory.java:706)
at org.apache.commons.httpclient.HttpConnection.open(HttpConnection.java:706)
at org.apache.commons.httpclient.HttpMethodDirector.executeWithRetry(HttpMethodDirector.java:386)
at org.apache.commons.httpclient.HttpMethodDirector.executeMethod(HttpMethodDirector.java:170)
at org.apache.commons.httpclient.HttpClient.executeMethod(HttpClient.java:396)
at org.apache.commons.httpclient.HttpClient.executeMethod(HttpClient.java:324)
at com.ca.technology.iclient.iclutil.httpRequest(IclUtil.java:1256)
... 40 more
ERROR 2010-06-01 15:08:10,046 [http-0.0.0.0-8080-2] [com.ca.eiam.jpz.PozFactory] setFailover(hostname) - EEM server not able
ERROR 2010-06-01 15:08:10,046 [http-0.0.0.0-8080-2] [com.ca.eiam.jpz.PozFactory] setFailover(hostname) - EEM server establish
```

This timeout will then trigger a response to attach to the Backend CA EEM server as shown below

```
at org.jboss.security.plugins.JaasSecurityManager.defaultLogin(JaasSecurityManager.java:572)
at org.jboss.security.plugins.JaasSecurityManager.authenticate(JaasSecurityManager.java:506)
at org.jboss.security.plugins.JaasSecurityManager.isValid(JaasSecurityManager.java:315)
at org.jboss.web.tomcat.security.JBossSecurityMgrRealm.authenticate(JBossSecurityMgrRealm.java:230)
at org.jboss.web.tomcat.security.FormAuthenticator.authenticate(FormAuthenticator.java:256)
at com.optinuity.c2o.server.C2OFormAuthenticator.authenticate(C2OFormAuthenticator.java:93)
at org.apache.catalina.authenticator.AuthenticatorBase.invoke(AuthenticatorBase.java:391)
at org.jboss.web.tomcat.security.JaccContextValve.invoke(JaccContextValve.java:59)
at org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:126)
at org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:105)
at org.jboss.web.tomcat.tc5.sso.ClusteredSingleSignon.invoke(ClusteredSingleSignon.java:366)
at org.apache.catalina.core.StandardEngineValve.invoke(StandardEngineValve.java:107)
at org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:148)
at org.apache.coyote.jk.common.HandlerRequest.invoke(HandlerRequest.java:385)
at org.apache.jk.common.ChannelSocket.invoke(ChannelSocket.java:748)
at org.apache.jk.common.ChannelSocket.processConnection(ChannelSocket.java:678)
at org.apache.jk.common.SocketConnection.runIt(ChannelSocket.java:871)
at org.apache.tomcat.util.threads.ThreadPool$ControlRunnable.run(ThreadPool.java:684)
at java.lang.Thread.run(Unknown Source)
Caused by: java.net.ConnectException: Connection timed out: connect
at java.net.PlainSocketImpl.socketConnect(Native Method)
at java.net.PlainSocketImpl.doConnect(Unknown Source)
at java.net.PlainSocketImpl.connectToAddress(Unknown Source)
at java.net.PlainSocketImpl.connect(Unknown Source)
at java.net.SocksSocketImpl.connect(Unknown Source)
at java.net.Socket.connect(Unknown Source)
at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
at sun.reflect.NativeMethodAccessorImpl.invoke(Unknown Source)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(Unknown Source)
at java.lang.reflect.Method.invoke(Unknown Source)
at org.apache.commons.httpclient.protocol.ReflectionSocketFactory.createSocket(ReflectionSocketFactory.java:139)
at org.apache.commons.httpclient.protocol.DefaultProtocolSocketFactory.createSocket(DefaultProtocolSocketFactory.java:124)
at org.apache.commons.httpclient.HttpConnection.open(HttpConnection.java:706)
at org.apache.commons.httpclient.HttpMethodDirector.executeWithRetry(HttpMethodDirector.java:386)
at org.apache.commons.httpclient.HttpMethodDirector.executeMethod(HttpMethodDirector.java:170)
at org.apache.commons.httpclient.HttpClient.executeMethod(HttpClient.java:396)
at org.apache.commons.httpclient.HttpClient.executeMethod(HttpClient.java:324)
at com.ca.technology.iclient.iclutil.httpRequest(IclUtil.java:1256)
... 42 more
ERROR 2010-06-01 15:43:51,937 [TP-Processor3] [com.ca.eiam.jpz.PozFactory] setFailover(hostname) - EEM server not able to
established connection with server
ERROR 2010-06-01 15:43:51,937 [TP-Processor3] [com.ca.eiam.jpz.PozFactory] setFailover(hostname) - EEM server established
connection during attachPoz
```

As you can see in the example above, it failed to establish connection with the primary CA EEM server and re-attached connection to the Backend Server.

If both CA EEM servers were down, then login will fail.