Hisense

海信集团企业信息门户系统
集成规范

二〇一四年　三月

编写	信息技术管理部	日期	2014-3-20
校对		日期	

审批		日期	
批准		日期	

日期	版本	说明	作者
2014-3-20	1.0	初版包含：单点登录集成规范、统一待办集成规范、门户系统集成 UI 规范	
2014-5-5	2.0	增加 LDAP 集成规范，补充 UI 规范素材	
2014-6-25	3.0	修订 HTTP Header 集成方式描述 增加业务系统页面集成规范	
2014-9-18	4.0	补充业务系统会话管理，JSESSIONID 命名要求及业务系统发布上下文根要求	

目 录

一、 总体概述

1. 编写目的

编写此文档的目的是为海信集团企业信息门户建设及业务系统集成提供统一的规范，为后续系统建设、开发、实施提供依据。

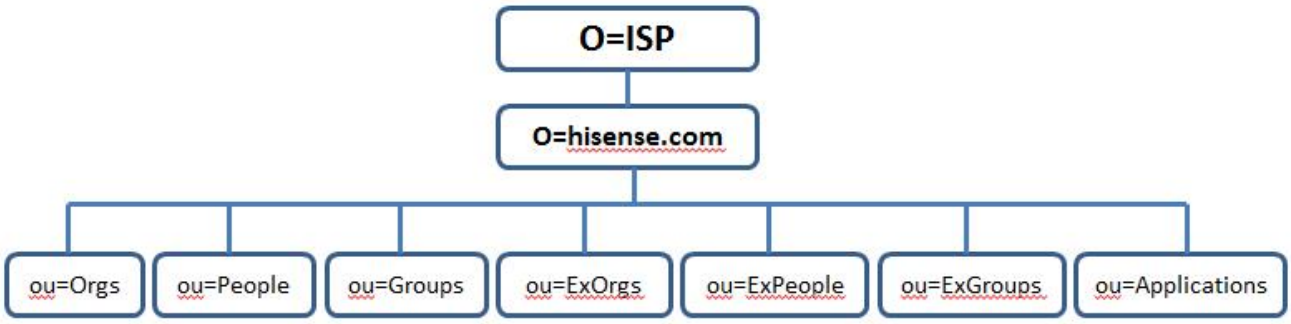
2. 术语

LDAP	轻量目录访问协议，英文全称是 Lightweight Directory Access Protocol
SSO	单点登录，英文全称 Single Sign On。SSO 是在多个应用系统中，用户只需要登录一次就可以访问所有相互信任的应用系统
WebService	Webservice 是一个平台独立的，松耦合的，自包含的、基于可编程的 web 的应用程序，可使用开放的 XML 标准来描述、发布、发现、协调 和配置这些应用程序，用于开发分布式的互操作的应用程序
XML	用于标记电子文件使其具有结构性的标记语言，可以用来标记数据、定 义数据类型，是一种允许用户对自己的标记语言进行定义的源语言。 XML 是标准通用标记语言(SGML) 的子集，非常适合 Web 传输。XML 提供统一的方法来描述和交换独立于应用程序的结构化数据。

二、 LDAP 集成规范

1 LDAP 架构设计

海信集团企业信息门户系统的 LDAP 使用 IBM Tivoli Diectory Server 软件产品为基础，与主数据源 SUN ONE LDAP 保持完全一致的架构设计，如下



第一层

【O=ISP】

说明：海信集团门户目录的根节点

第二层

【o=hisense.com】

说明：

第三层

1）【ou=Orgs】：海信集团本部部门及各级直属公司、部门

2）【ou=People】：海信集团所有内部员工

3）【ou=Groups】：该节点中存储海信集团全局系统用户组

4）【ou=Applications】：该节点中存储海信集团应用系统账号

2 LDAP 属性设计

LDAP 测试系统地址：172.16.35.84:389

类型：SunOne Directory

帐号：uid=ea,ou=applications,o=hisense.com,o=isp

密码：Ea12345678

群组属性：（检索该组中的用户，当用户属于该组时，同步用户）

用户组名称和 DN：

cn=ea,ou=groups,o=hisense.com,o=isp

群组成员属性：uniqueMember

用户基准 DN：ou=People,o=hisense.com,o=isp

过滤条件: (objectClass=person)

用户唯一标识：uid

最近修改时间属性： modifytimestamp

记录唯一标识属性： entryid

用户显示名属性：cn

用户登录名属性：uid

排序号属性：displayid（逆向排序，当 displayid 一样时，使用 uid 升序）

所属部门关联属性：departmentNumber

邮箱地址属性：mail

办公室电话属性：telephonenumber

传真号码属性：facsimileTelephoneNumber

移动电话属性：mobile

部门基准 DN：ou=orgs,o=hisense.com,o=isp

筛选条件：

(&(objectClass=organization)(!(departmentNumber=other*))(!(departmentNumber=qz*)))

部门记录唯一标识属性：o

部门显示名属性：displayName

部门关联属性：departmentNumber

父部门关联属性：parentdepartment

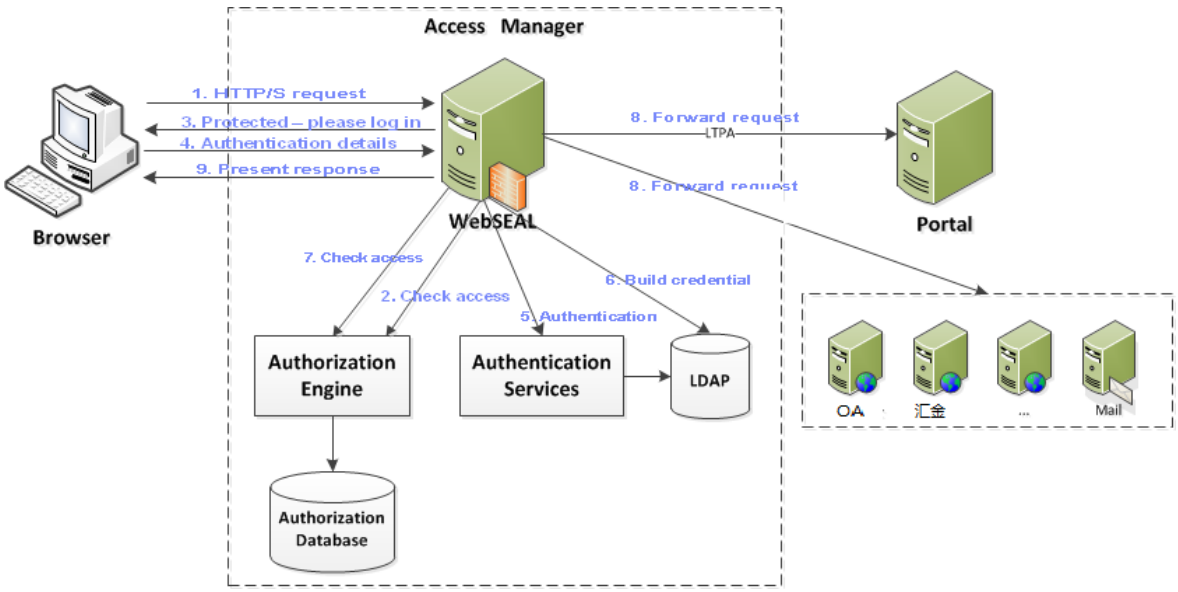
部门排序号属性：displayid（逆向排序，当 displayid 一样时，使用 departmentNumber 升序）

三、 单点登录集成规范

1 概述

单点登录（Single Sign On），简称为 SSO，是目前比较流行的企业业务整合的解决方案之一。SSO 的定义是在多个应用系统中，用户只需要登录一次就可以访问所有相互信任的应用系统。

2 TAM 单点认证过程



1、终端用户通过浏览器访问门户（或其他应用系统），该用户请求被访问网关（WebSEAL）所拦截。

2、访问网关与授权引擎（Authorization Engine）交互判断用户请求是否合法和访问权限。

3、用户访问了受保护的资源，访问网关要求用户进行登录认证。

4、用户填写认证信息并提交给访问网关。

5、访问网关把用户提交的认证信息提交给认证服务（Authentication Services），认证服务读取 LDAP 目录校验用户认证信息的合法性。

6、用户认证信息正确，访问网关绑定用户凭据。

7、访问网关再次与授权引擎进行交互，识别用户的访问权限。

8、访问网关把用户请求提交给门户（或其他应用系统），门户（或其他应用系统)再次对用户的信息进行合法验证 ,认证通过把请求的资源返回给访问网关。

9、访问网关把请求的资源返回给用户，当用户从门户或直接访问其他应用

系统时，用户就不需要再次进行登录认证。

3 常用 SSO 方法

通过 TAM 实现用户单点集成方式有以下三种方式：

1、基于 LTPA(LTPA Token)认证;

2、基于 HTTP Header 认证；

3、基于表单(Form)认证;

3.1 基于 LTPA(LTPA Token)认证

适用目标系统

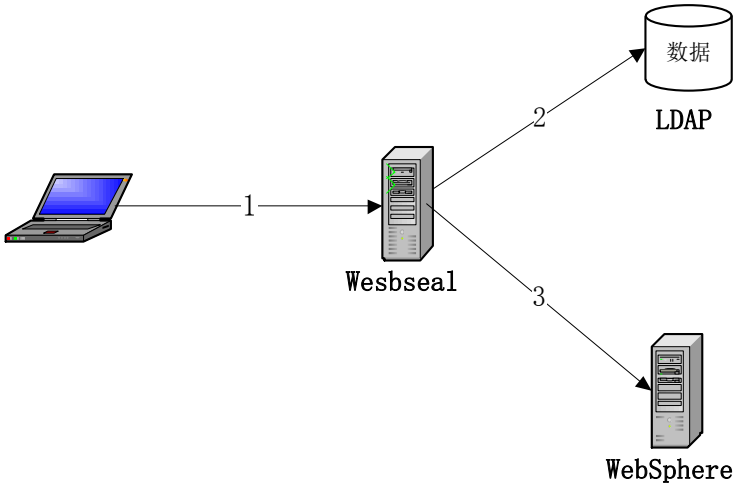
LTPA 是 IBM 提供的基于 cookie 的轻量级的认证方式，如果需要实现 SSO 的环境为 IBM 提供的各种中间件，那么使用 LTPA 将是最佳的方式，例如：Domino 平台系统和基于 WAS 认证的 WebSphere 平台系统。

认证过程

过程说明：

首先需要 Domino 或基于 WAS 的服务与 TAM 的 Webseal 上配置基于 LTPA 的信任关系，经过配置后的服务之间建立了信任，当访问 Webseal 认证成功后生成一个 LTPA 的 Token，并将请求转发到 Domino 或 WAS 端，Domino 或 WAS 收到请求后，发现此请求含有 LTPA 的 Token，因为之前已经配置了它和 Webseal 的信任关系，所以不再要求进行认证，直接将请求的响应返回。

下面以 WAS 和 Webseal 来简单说明一下 LTPA 信任的认证过程:



LTPA 认证

(1) 用户发出一个 SSO 的 URL 请求访问部署在 WAS 上的 Web 应用(此 WAS 与 WebSeal 配置完 SSO)，此请求被 Webseal 拦截，Webseal 定向到登录页面，要求输入用户/密码进行认证;

(2) Webseal 根据提交的用户/密码在 LDAP 数据库中进行用户认证;

(3) Webseal 认证成功后生成一个 LTPA 的 Token，并将请求转发到 WAS 端，WAS 收到请求后，发现此请求含有 LTPA 的 Token，因为之前已经配置了它和 Webseal 的信任关系，所以 WAS 不再要求进行认证，直接将请求的响应返回，部署在 WAS 的 WEB 应用可获取认证成功的用户，然后 web 应用判断此用户访问权限。

门户系统实施内容

1、门户系统在 Websphere 控制台导出 Ltpa key，并将 key 文件及密码提供给业务系统；

2、根据第三方系统系统的信息，完成单点测试工作，单点配置命令如下：

参数注释：

server task instance_name-webseald-host_name create –t type –h host_name –p port -A –F keyfile –Z password -c all –x -s –f junction_point

参考如下：

server task default-webseald-websealdev01.hisense.com create -t tcp -h portaldev01.hisense.com -p 10039 -A -F /opt/pdweb/key/ltpa20140306.key -Z Hisense3 -c all -x -s -f /wps

参数注释：

- instance_name-webseald-host_name : webseal 实例的服务全名，instance_nam 表示是 webseal 实例名，host_name 表示 webseal 实例所在的主机名，也可以通过 server list 命令查询；
- type ：junction 类型，为 tcp、tcpproxy、ssl、sslproxy、local 中的其中一种；
- port： 第三方服务的端口号，junction 类型为 tcp 时默认端口为 80，ssl 默认端口为 443；
- keyfile：ltpa key 文件在 webseal 服务器上的存放路径；
- password：导出 key 文件时设置的密码；
- junction_point：junction 的名称

1、 根据第三方系统需要的账户信息，创建对应的 junction；

2、 完成生产环境单点集成工作；

第三方应用系统实施内容

1、 第三方应用系统提供以下信息给门户系统，便于单点集成使用，举例如下：

名称	**说明**
IP	应用系统的访问的 IP 地址和域名，例如： 172.16.35.59/koadev.hisense.com

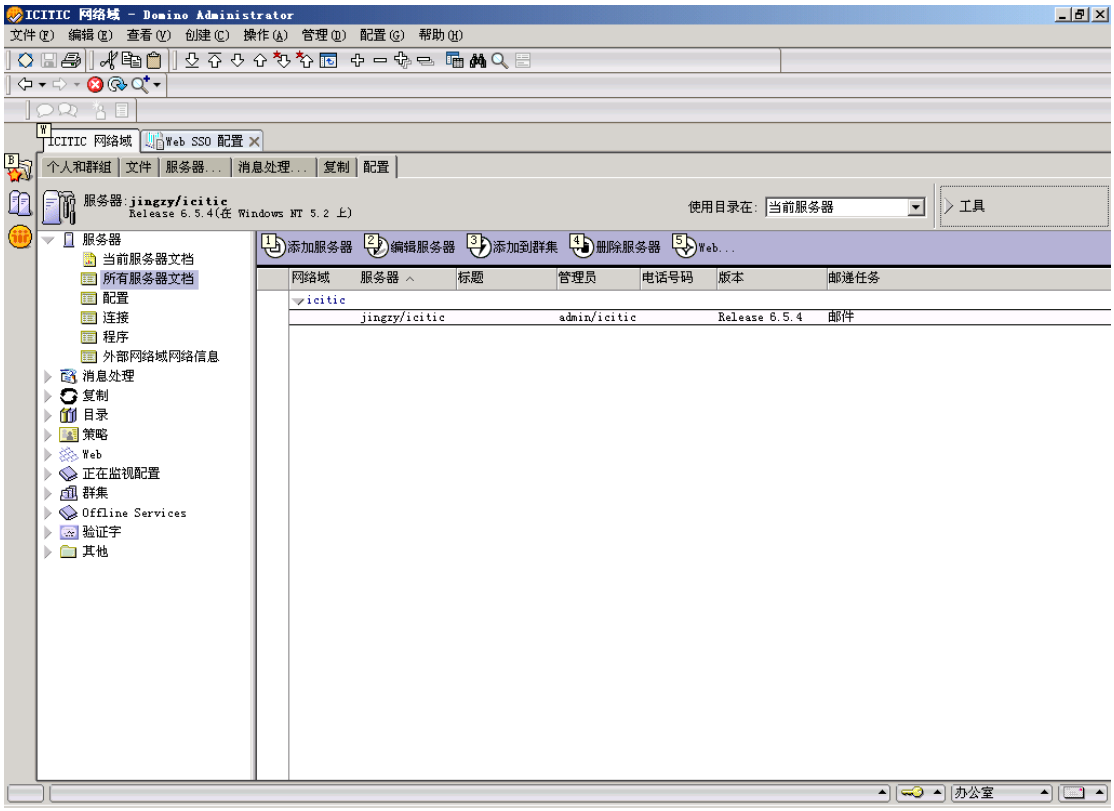
端口	应用系统的访问时的端口号，例如：80
访问协议	http

2、 第三方应用系统从门户系统获取 LTPA key 和密码；

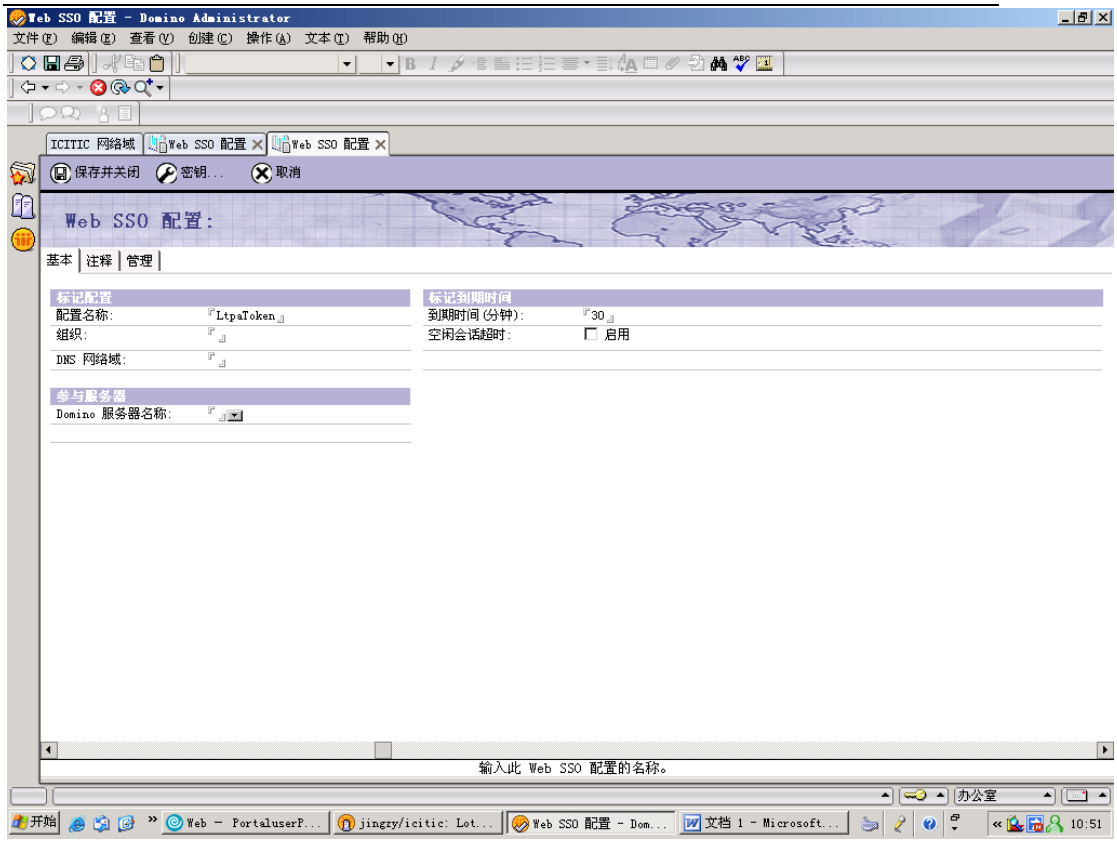
3、 配置 WebSSO（以 Domino 为例）

进入 Lotus 管理控制台，在 Domino 的管理控制台中,选择配置 tab，在导航面板,

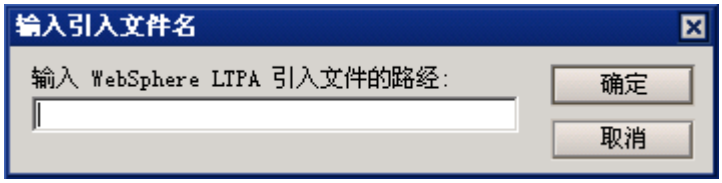
选择所有服务器文档，进入到如下界面中，点击 WebSSO



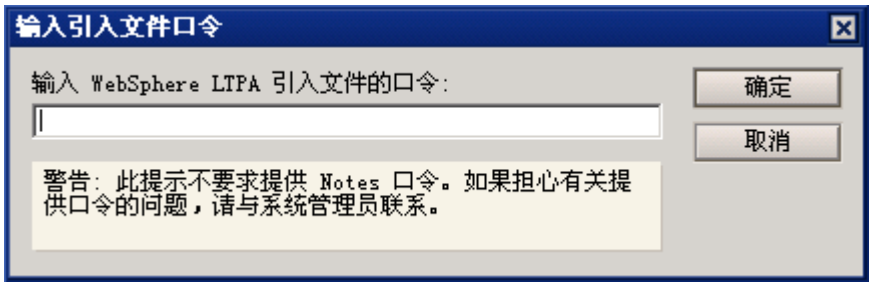
点击 WebSSO 配置，进入 WebSSO 设置，点击密钥，引入



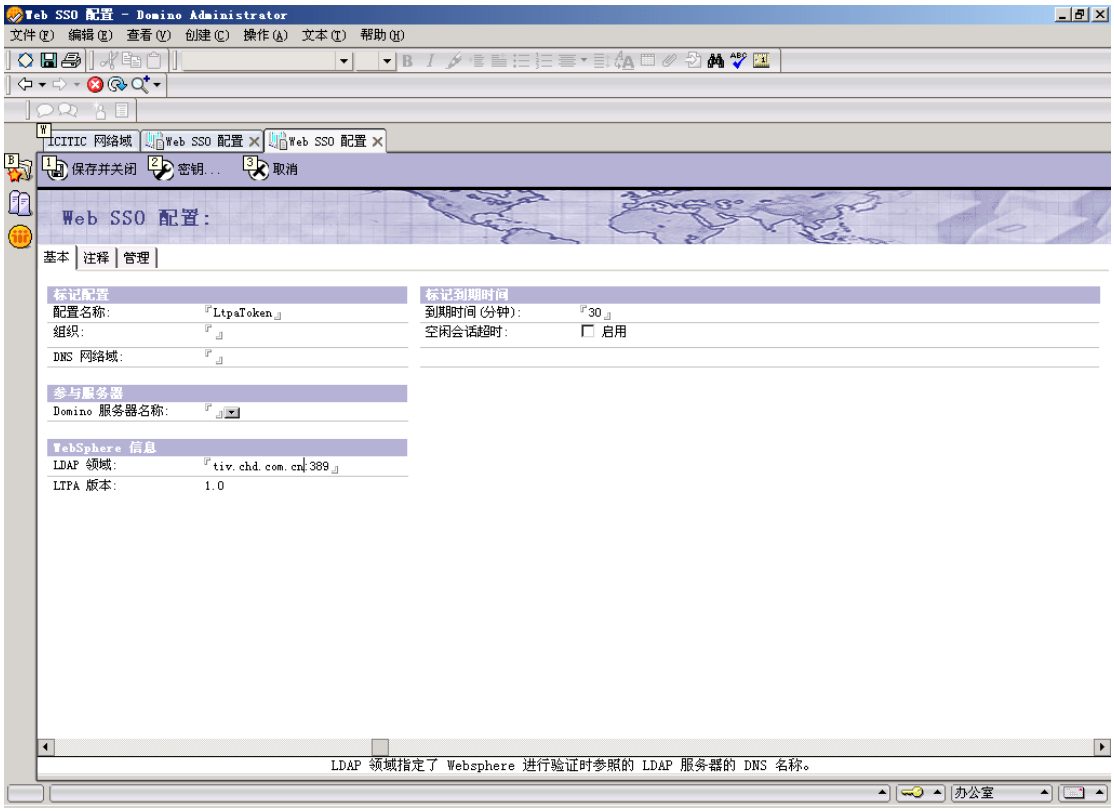
输入密钥路径（本地路径）

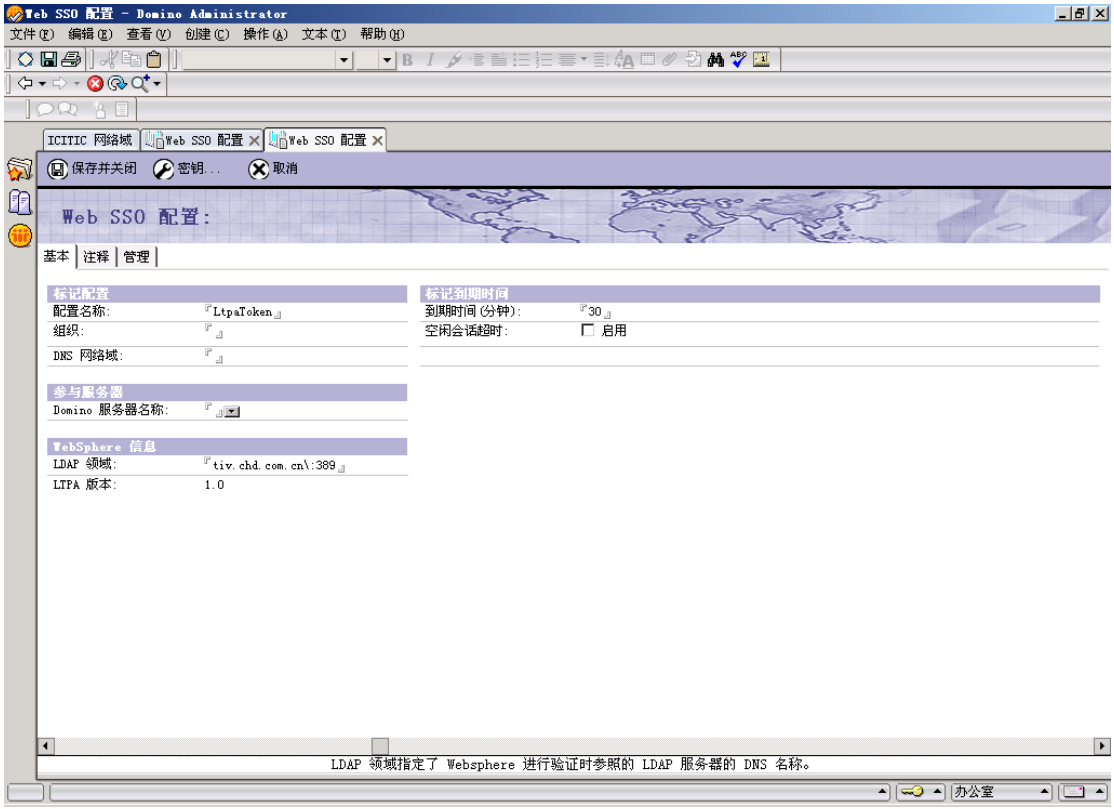


输入密钥密码（门户系统提供的文件密码）



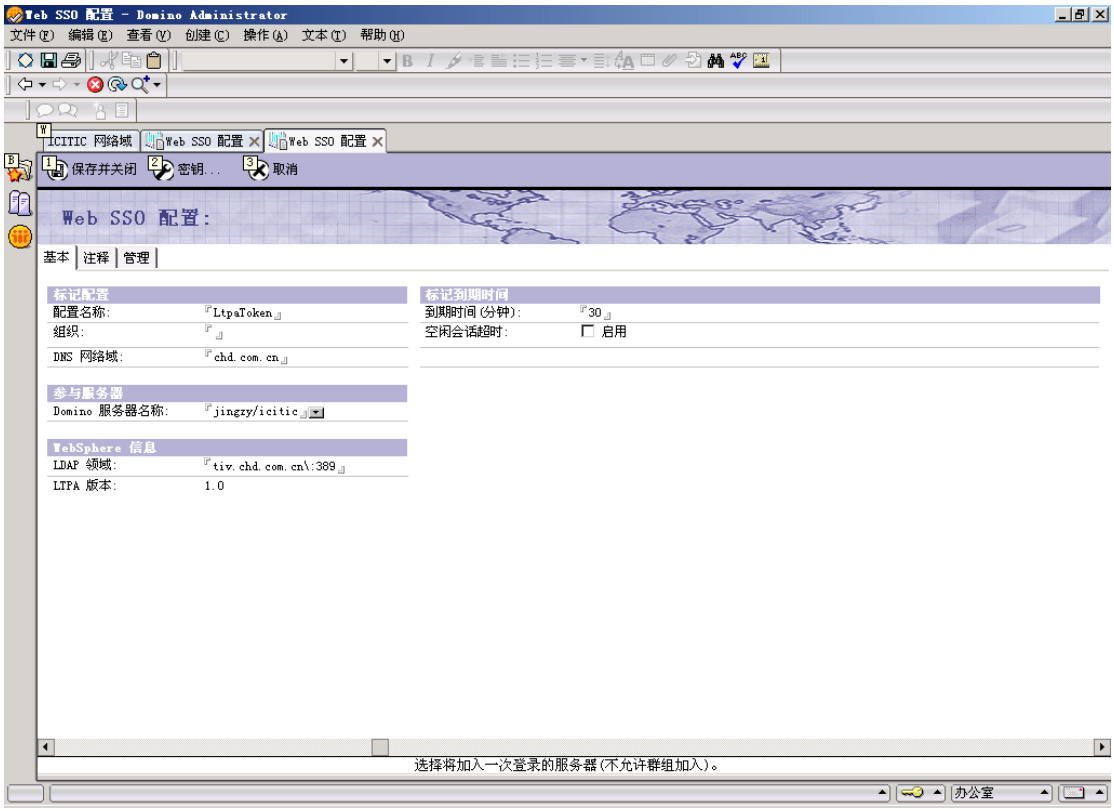
设置 LDAP 领域，在 LDAP 领域中的 “:”（冒号）前面要添加一个\，





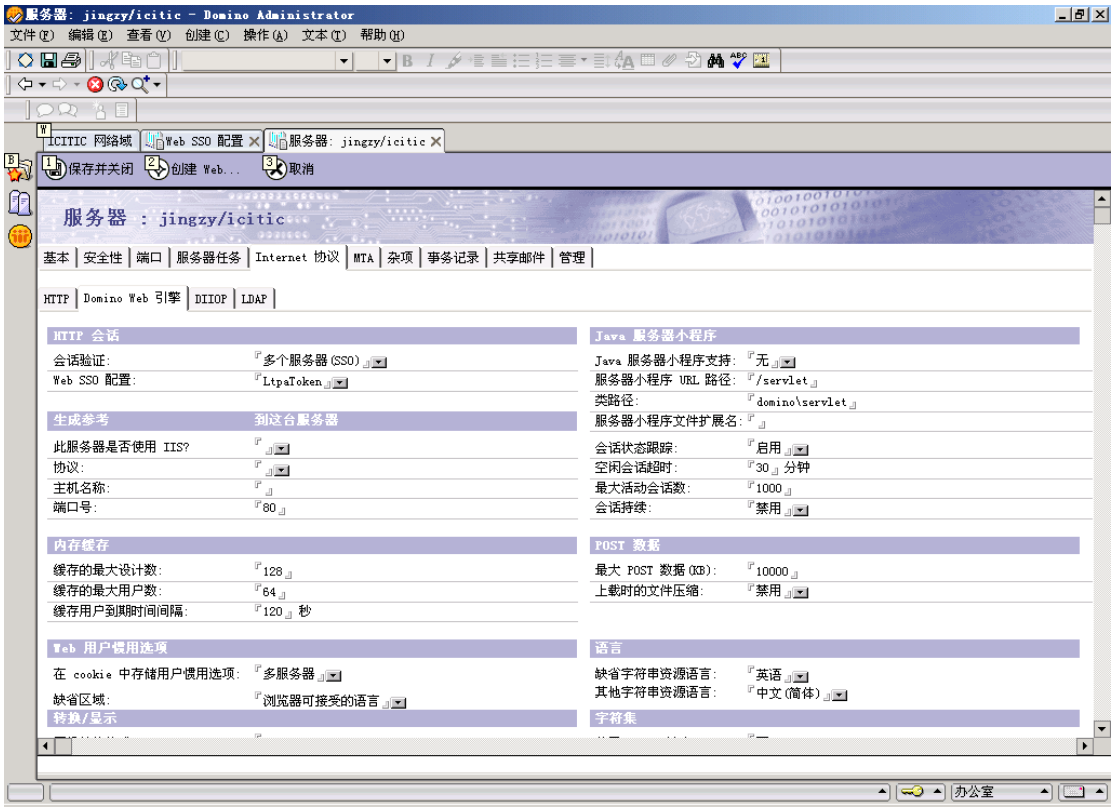
设置 Domino 服务器名称选择要加入 SSO 的服务器。

设置 DNS 网络域：.hisense.com



选择服务器——〉internet 协议——〉DominoWeb 引擎

设置会话验证为多服务器，WebSSO 选择刚才创建的 LTPA Token



4、 配置用户信息

Domino 系统的用户全限定名称和组织结构与门户系统规划不一致，则必须修改 OA 系统用户的用户名。

具体做法：

1） 在 OA 系统中为每一个"登录名"的属性中新添加一个属性“用户名”，形式为 uid=userid/ou=People/o=hisense.com/o=isp 和用户的 UID。

添加的步骤：

A. 在 Domino 的管理控制台,打开个人文档

B. 在基本表格中,找到登录名字段

C. 在登录名称的列表中增加用户相对应的 LDAP DN，注意需要用"/"替换","，这是 Domino 要求的格式

比如:

Domino 中的登录名为:

zhangsy/Hisense

zhangsy

zhangsy 在 LDAP 中的用户 DN 为 uid=zhangsy,ou=People,o=hisense.com,o=isp，那么在这里需要输入 uid=zhangsy/ou=People/o=hisense.com/o=isp 和 zhangsy，最后显示为下面的形式:

zhangsy/Hisense

zhangsy

uid= zhangsy/ou=People/o=hisense.com/o=isp

zhangsy

其中用户的 UID 必须放在名称的最后一行

2） 修改用户名的搜索属性

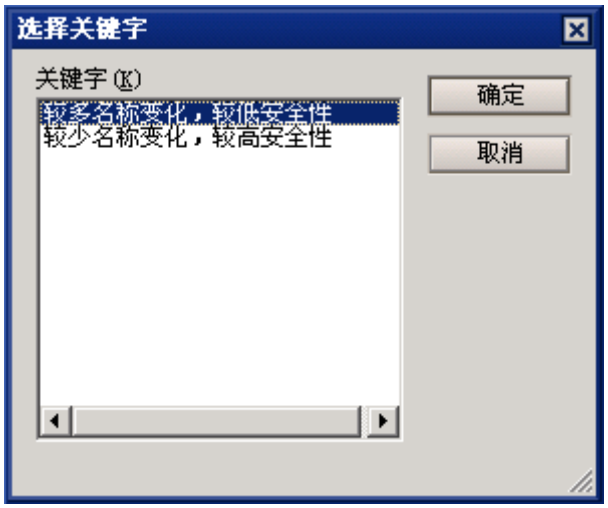
A. 在 Domino 的管理控制台中，选择“配置”页签；

B. 在导航面板，选择当前服务器文档；

C. 选择“安全”页签；

D. 选择 internet 访问，定位到 internet 认证；

E. 将当前的值改为“较多名称变化，较低安全性”；



F. 保存当前配置,并重新启动服务器。

3.2 基于 HTTP Header 认证

适用目标系统

1、适用于可改造认证模块的系统

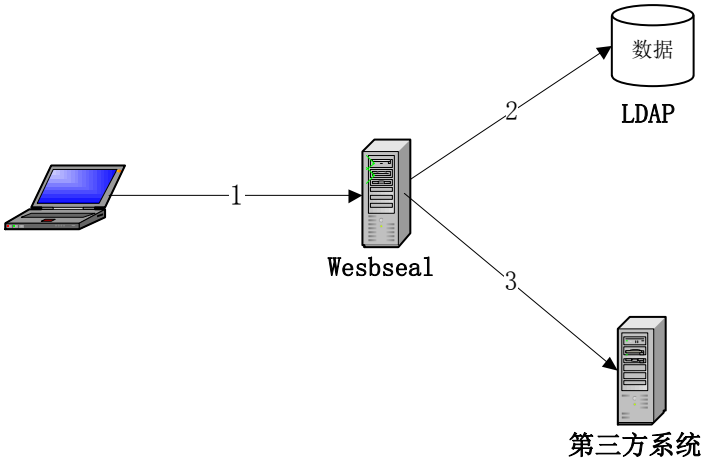
2、第三方应用系统用户名与门户相同，或者存在一个与门户中一致的唯一标示。

认证过程

过程说明：

当访问 Webseal 认证成功后，Webseal 通过 Http header 向第三方系统提供帐号信息(例如登陆用户名)，第三方系统获取此账户信息后，利用此账号信息自行进行用户授权或者认证和授权

下面以 Http header 认证方式来简单说明一下认证过程:



header 认证

(1) 用户发出一个 SSO 的 URL 请求访问部署在第三方系统上的 Web 应用(此 web 应用与 WebSeal 配置 header 的 SSO)，此请求被 Webseal 拦截，Webseal 定向到登录页面，要求输入用户/密码进行认证;

(2) Webseal 根据提交的用户/密码在 LDAP 数据库中进行用户认证;

(3) Webseal Webseal 通过 Http header 向第三方系统提供帐号信息(例如登陆用户名)，第三方系统获取此账户信息后，利用此账号信息自行进行用户授权或者认证和授权。

门户系统实施内容

1、根据第三方系统系统的信息，完成单点测试工作，单点配置命令如下：

参数注释：

server task instance_name-webseald-host_name create –t type –h host_name –p port -c iv_user -s -f junction_point

参考如下：

server task default-webseald-websealdev01.hisense.com create -t tcp -s -j -c iv_user -h cm.hisense.com -p 80 -f /cm

参数注释：

- instance_name-webseald-host_name : webseal 实例的服务全名，instance_nam 表示是 webseal 实例名，host_name 表示 webseal 实例所在的主机名，也可以通过 server list 命令查询；
- type ：junction 类型，为 tcp、tcpproxy、ssl、sslproxy、local 中的其中一种；
- port： 第三方服务的端口号，junction 类型为 tcp 时默认端口为 80，ssl 默认端口为 443；
- junction_point：junction 的名称

3、 根据第三方系统需要的账户信息，创建对应的 junction；

4、 完成生产环境单点集成工作。

第三方应用系统实施内容

1、第三方应用系统提供以下信息给门户系统，便于单点集成使用，举例如下：

名称	**备份**
IP	应用系统的访问的 IP 地址和域名，例如：172.16.35.94/cm.hisense.com

端口	应用系统的访问时的端口号，例如：80
访问协议	http
登陆地址	登陆时访问的地址，例如：http(s):// cm.hisense.com
公钥证书	当访问协议为 https 时，需要提供公共秘钥部分

2、提供需要在 Http header 获取帐号信息列表(前提：这些账号信息在 webseal 中都存在)，例如：用户名、部门名称等，获取方式如下：

String username = request.getHeader("iv-user");

增加 IP 验证及用户名加密（用户名采用 Base64 加解密）后代码如下：

```
//引入 jar 包（开发时与信息部所取）
<%@ page import="weaver.login.*"%>
//获取 request 中的用户名信息：
String username = “”;
String encryptname = request.getHeader("encryptname");  //获取 request header 中的加密用户名字段
username= Base64Coder.decrypt(encryptname);//解密用户名
//下边标记蓝色的代码，获取邮件别名以及是否使用别名标识，为邮件系统专用
String  encryptMail = request.getHeader(" encryptMail ");  //获取加密邮件
String  loginalias  = request.getHeader(" loginalias");  //获取邮件别名
if(loginalias!=null & !loginalias.equals("")){ //判断邮箱别名不为空
    username  =  loginalias; //使用别名认证
```

```
        }else{
            if(encryptMail  !=null & !encryptMail.equals("")){
              username  = Base64Coder.decrypt(encryptMail );
            }
        }
        //获取 request 中的 WebSEAL ip 地址 ,172.16.64.128、129、142 为 webseal
的 IP 地址
        String websealip = request.getRemoteAddr();
        if (websealip.equals("172.16.64.142") ||
websealip.equals("172.16.64.128") || websealip.equals("172.16.64.129")) {
        //以下为业务处理逻辑
            …
        }
```

3.3 基于表单(Form)认证

适用目标

1、第三方系统登陆时的认证模块改造困难或无法改造；

2、第三方系统提供的表单登录页面必须符合以下要求：

a)系统登录页面不能包含随机或动态参数变量；

b)系统为单点登录集成提供登录页面必须包含标准的 form 表单项，至少包括表单名，action 地址，用户名，密码；

认证过程

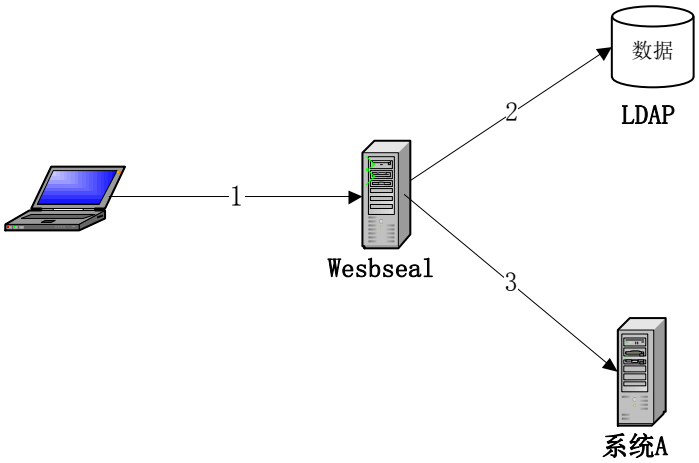
过程说明：

首先需要通过表单进行单点登录认证的第三方系统在登录的时候均有一个登录页面，Webseal 可以对该登录页面上需要进行提交的表单中的内容设置自动填表策略；

该策略工作的方式：当用户通过单点地址访问第三方系统的登陆页面时，如果该用户有权限访问该页面，该策略首先确定该页面是否存在登陆的表单，如果存在就将策略里面定义的 username, password 提交给登陆表单定义的目标。

第三方应用系统接收到提交的用户信息后，对用户进行认证，具体的第三方应用系统的权限由第三方应用系统自己管理。统一认证系统只负责判断用户是否允许访问资源以及传递第三方应用系统登陆表单所需要的用户信息。

下面以表单(Form)认证方式来简单说明一下认证过程:



表单认证

(1) 当用户发出一个 SSO 的 URL 请求到系统 A 时，Webseal 拦截此请求，并要求输入帐号信息，用户输入 Webseal 的帐号信息并提交；

(2) Webseal 根据提交的用户/密码在 LDAP 数据库中进行用户认证；

(3) Webseal 认证成功后，跳转至系统 A 的登陆页面，由于 Webseal 与系

统 A 配置了表单认证，Webseal 的自动填表策略将 GSO 中配置的系统 A 账户信息提交至系统 A 的登陆页面的表单中，系统 A 的根据提交的表单数据进行用户认证。

4 海信集团应用系统单点登录

应用系统特点

1）海信集团应用系统的用户信息均源自 UUM 系统，可保证所有系统中均存在一个相同的唯一标识。

2）海信集团应用系统均使用 UUM 系统的 LDAP 进行认证，均使用相同的用户名和密码。

单点方式

海信集团企业信息门户系统与各应用系统使用 **LTPA 方式**和 **HTTP Header 方式**的单点登录。

门户系统是集成后所有应用系统的统一入口，登录门户系统后，从门户系统跳转到业务系统无需再次输入用户名、密码进行认证；但是从原有业务系统的登录入口进入，是无法实现门户系统与业务系统单点登录的。

5 关于上下文根

对于与门户系统（webseal）进行单点登录集成的业务系统，在中间件上发布应用时，要求使用非默认上下文根（即不能以“/”作为应用系统的上下文根）

原因：

1、 webseal 自身以“/”作为根目录；

2、 对于相同架构（资源目录相同）的产品部署的多套应用系统，与门户

系统集成时，此种情况只能创建非透明 junction，使用 jmt 配置表进行资源目录映射，相同名称的资源目录会导致加载 jmt 失败；

3、后端业务系统因安全审计需求，需要获得客户端真实 IP，必须与 webseal 配置单点时使用透明 junction（也就是必须 webseal 上的 junction 名称与业务系统的上下文根一致），否则后端只能获取到 webseal 的 ip 地址。

6 关于会话管理

与门户系统实现单点登录集成或者内容嵌入集成的业务系统，应保持唯一的 JSESSIONID 名称，否则会因为 JSESSIONID 冲突儿导致单点失败。

设置方式如下（以 WAS 为例）：

a、server 级别的 cookie 命名

进入 was 控制台，服务器-》WebSphere Application Server-》选择 server-》会话管理-》会话跟踪机制 中，点击“启用 cookie”，在 cookie 配置页面，将默认的 cookie 名"JSESSIONID"改为业务系统唯一的 cookie 名。然后“确定”，“保存”。所有的server进行同样的操作，同一个业务系统的所有server使用同一个cookie

名。重启 server 生效。见下图

b、应用级别的 cookie 命名

进入 was 控制台，应用程序-》应用程序类型-》WebSpere 企业应用程序-》选择应用-》会话管理-》会话跟踪机制 中，点击“启用 cookie”，在 cookie 配置页面 ,将默认的 cookie 名"JSESSIONID"改为应用程序唯一的 cookie 名。然后“确定”，“保存”。同一个 was 上部署的多个应用应保持 cookie 名唯一。重启 server 生效。见下图

C、代码级的 cookie 命名

对于企业应用中，有采用同一产品进行多个应用部署的情况，此情况下如果出现会话冲突，就需要在代码中将相同的 JSESSIONID 进行唯一命名。

7 关于会话超时

门户系统会话简介

门户系统实施完成后，包括以下系统会话：

1、Webseal 会话：

Webseal 为 TAM 产品中的反向代理和认证组件，所有的应用系统都通过 Webseal 服务器代理访问。

Webseal 会话可视为整个门户系统的会话

2、应用系统会话，WebSeal 代理的各应用系统的会话，包括：

- Portal 服务器会话
- WAS 服务器会话
- 第三方应用系统会话

WebSeal 会话和应用系统会话关系

WebSeal 会话时间大于应用系统会话时间

WebSeal 会话时间大于应用系统会话时间的情况下，场景如下：

如果通过 WebSeal 访问应用系统，应用系统超时后，会提示应用系统超时；但是 WebSeal 的会话不受该应用系统影响，WebSeal 的会话不会超时；如果现在从 WebSeal 再次发起单点登录到该应用系统的请求，还是可以继续登录该应用系统进行使用。

WebSeal 会话时间小于应用系统会话时间

WebSeal 会话时间小于应用系统会话时间的情况下，场景如下：

如果通过 WebSeal 访问应用系统，WebSeal 超时，则应用系统随即也会超时无法认证访问。

门户系统集成会话时间设置要求

WebSeal 和各应用系统的超时时间设置为相同。

8 其他要求

1、 集成的业务系统中应避免使用绝对路径；

2、 使用门户系统 webseal 单点登录，进入业务系统应保持 webseal 域名，避免强跳转。