将ECE与12.0及更高版本中的PCCE集成

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

术语

必备步骤

集成步骤

- 步骤1:配置SSL证书
  - 步骤 1.1生成证书
  - 步骤 1.2将证书绑定到网站
- 第二步：配置分区管理员SSO
  - 步骤 2.1获取Active Directory(AD)证书并创建密钥库。
  - 步骤 2.2使用AD轻型目录访问协议(LDAP)访问信息配置ECE。
- 第三步：验证配置文件
- 第四步：将ECE添加到PCCE库存
  - 步骤 4.1将ECE Web服务器证书上传到Java密钥库
  - 步骤 4.2将ECE数据服务器添加到库存
  - 步骤 4.3将ECE Web服务器添加到库存
- 第五步：将ECE与PCCE集成
- 第六步：验证ECE集成

故障排除

- ECE上的文件名和位置
- PCCE上的文件名和位置
- 跟踪级别配置
- 日志文件收集

相关信息

简介

本文档介绍将企业聊天和电子邮件(ECE)与Packaged Contact Center Enterprise(PCCE)集成到版本12.0及更高版本中的步骤

先决条件

要求

Cisco 建议您了解以下主题：

- 企业聊天和电子邮件(ECE)12.x
- 套装联络中心企业版(PCCE)12.x

使用的组件

本文档中的信息基于以下软件版本：

- 欧洲经委会12.5(1)
- PCCE 12.5(1)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

PCCE版本12.0引入了新的管理界面，称为单一管理平台(SPOG)。现在，几乎所有的联系中心及相关应用都在此界面中执行。为了正确集成ECE和PCCE，您必须完成此集成独有的几个步骤。本文档将指导您完成此流程。

术语

本文档中使用了这些术语。

- 企业聊天和电邮(ECE)- ECE是一种产品，允许以与语音呼叫相同的方式将电邮和聊天请求路由到联系中心座席。
- 单一平台(SPOG)- SPOG是PCCE管理在12.0版及更高版本中执行的方式。SPOG是对在12.0之前的版本中使用的CCE管理工具的完全重写。
- 证书颁发机构(CA) — 根据公钥基础设施(PKI)模型颁发数字证书的实体。

  您可以遇到两种类型的CA。

  - 公共CA — 公共CA是大多数浏览器和操作系统都包含其根证书和中间证书的CA。一些常见的公共CA包括IdenTrust、DigiCert、GoDaddy和GlobalSign。
  - 专用CA — 专用CA是公司内部存在的专用CA。某些私有CA由公共CA签名，但大多数情况下这些私有CA是独立的CA，它们颁发的证书仅受该组织中的计算机信任。

  在这两种CA类型中，有两种类型的CA服务器。

  - 根CA服务器 — 根CA服务器签署自己的证书。在标准的多层PKI部署中，根CA处于离线状态且不可访问。此模型中的根CA也只向另一个称为中间CA的CA服务器颁发证书。有些公司选择仅使用单层CA。在此模型中，根CA颁发证书供其他CA服务器之外的实体使用。
  - 中间CA服务器 — 中间或颁发CA服务器颁发证书供其他CA服务器之外的实体使用。
- Microsoft管理控制台(MMC)- Microsoft Windows附带的允许加载各种管理单元的应用程序。您可以使用管理单元构建用于服务器管理的自定义控制台。Windows中包含许多不同的管理单元。示例的简短列表包括证书、设备管理器、磁盘管理、事件查看器和服务。

- 网络负载均衡器(NLB) — 向具有通用物理名称的最终用户提供多个物理资源的设备或应用。NLB与Web应用和服务非常相似。NLB可以多种方式实施。当与ECE一起使用时，NLB的配置方式必须确保用户会话通过使用cookie-insert或等效方法返回到同一物理后端Web服务器。这称为带有cookie-insert的粘滞会话。粘滞会话只是指负载均衡器将用户会话返回到同一物理后端服务器进行所有交互的能力。
    - 安全套接字层(SSL)直通 — SSL直通是在最终用户设备和分配用户会话的物理Web服务器之间存在SSL会话的一种方法。由于HTTP会话始终以物理方式加密，因此SSL直通不允许进行Cookie插入。大多数NLB通过使用粘滞表支持带有SSL Passthrough的粘滞会话，粘滞表监控会话设置的服务器呼叫和客户端呼叫部分，并将唯一值存储在表中。当向NLB提交匹配这些值的下一个请求时，可以使用单臂表将会话返回到同一后端服务器。
    - SSL卸载 — 为SSL卸载配置NLB时，任何给定最终用户会话都存在两个SSL会话或隧道。第一个位于最终用户设备与在NLB上为网站配置的虚拟IP(VIP)之间。第二个地址位于NLB的后端IP与分配用户会话的物理Web服务器之间。SSL卸载支持cookie-insert，因为HTTP流已完全解密，而在NLB上，可以插入其他HTTP cookie并执行会话检查。当Web应用程序不需要SSL，而是出于安全考虑而执行SSL卸载时，通常使用SSL卸载。ECE的当前版本不支持在非SSL会话中访问应用。

必备步骤

在开始集成这两个系统之前，必须完成几个前提条件。

- 最低PCCE补丁级别
    - 版本12.0(1)- ES37
    - 版本12.5(1) — 基本功能当前没有最低要求
- 最低ECE补丁级别

  建议ECE运行最新的工程特别计划(ES)。

    - 版本12.0(1)- ES3 + ES3_ET1a
    - 版本12.5(1) — 基本功能当前没有最低要求
- 配置项目

  确保将ECE_Email、ECE_Chat和ECE_Outbound Media Routing Domains(MRD)与正确的应用实例相关联。

    - 对于PCCE 2000代理部署模型，应用实例是多通道并在部署PCCE时进行了预配置。
    - 对于PCCE 4000/12000代理部署模式，应用实例可以是任何名称，必须由执行集成的人员创建。最佳实践是使用{site}_{peripheral_set}_{application_instance}的形式。如果安装了PCCE，且站点名称为Main，外围设备设置为PS1，应用实例设置为Multichannel，则应用实例名称为Main_PS1_Multichannel。

注意：应用实例名称区分大小写。将ECE Web服务器添加到库存时，请确保正确键入名称。

集成步骤

本文件所有步骤的详细情况在欧洲经委会和太平洋经济合作委员会的文件中都有介绍，但这些步骤既没有列入清单，也没有列入同一文件。有关其他详细信息，请参阅本文档末尾包含的链接。

步骤1:配置SSL证书

必须生成证书供ECE Web服务器使用。您可以使用自签名证书，但使用CA签名证书通常更容易。自签名证书的安全性不低于CA签名证书，初始创建证书的步骤更少，但是当需要替换证书时，必须记住将新证书上传到所有PCCE管理数据服务器上的Java密钥库。如果使用CA签名的证书，则只需将根证书和中间证书（如果有）上传到密钥库。

如果部署中有多个Web服务器，则必须查看以下准则。配置网络负载均衡器所需的具体步骤不在本文档的讨论范围之内。如果需要，请联系您的负载均衡器供应商以获得帮助。

- 虽然不需要，但负载均衡器可大大简化实施
- 无论使用何种负载均衡器方法，访问每个Web服务器上的ECE应用都必须使用SSL
- 负载均衡器可以配置为SSL直通或SSL减负
- 如果选择SSL直通：
  - 您必须从一个服务器执行所有证书操作
  - 正确配置证书后，您必须导出证书并确保私钥包含在个人信息交换(PFX)文件中
  - 您必须将PFX文件复制到部署中的所有其他Web服务器，然后将证书导入IIS
- 如果选择SSL减负，则可以使用各自的SSL证书配置每个Web服务器

注意：如果您有多个Web服务器并且在Web服务器上选择SSL直通，或者如果您希望在所有服务器上都有一个通用证书，则必须选择一个Web服务器来执行第1步，然后将证书导入到所有其他Web服务器。
如果选择SSL卸载，则必须在所有Web服务器上执行这些步骤。您还必须生成要在负载均衡器上使用的证书。

步骤 1.1生成证书

如果您已经创建或获取了证书，则可以跳过此部分，否则请选择以下两个选项之一。

第 1 项.使用自签名证书

1. 导航到IIS Administration。
2. 在左侧的“连接”树中选择服务器名称。
3. 在中心窗格中找到Server Certificates，然后双击将其打开。
4. 从右侧的Actions窗格中选择Create Self-Signed Certificate...。
5. 在Create Self-Signed Certificate窗口中，在Specify a friendly name for the certificate:框中选择并输入名称。此名称是证书在下一个主要步骤的选择过程中的显示方式。此名称不需要与证书的公用名匹配，并且不会影响证书对最终用户的显示方式。
6. 确保在Select a certificate store for the new certificate: 下拉框中选择Personal。
7. 选择OK以创建证书。

8. 继续下一个主要步骤，将证书绑定到网站。

第 2 项.使用CA签名的证书

CA签名证书要求您生成证书签名请求(CSR)。CSR是文本文件，随后被发送到CA，并在其中签名，然后返回签名证书以及所需的CA证书，CSR已执行。您可以选择通过IIS管理或通过Microsoft管理控制台(MMC)执行此操作。IIS Administration（IIS管理）方法非常简单，它不需要特殊的知识，但只允许配置包含在证书的Subject（主题）属性中的字段并更改位长度。MMC需要执行其他步骤，并且您对有效CSR中所需的所有字段具有全面了解。强烈建议您仅在具有中等到专业证书创建和管理经验时使用MMC。如果您的部署要求通过多个完全限定名称访问ECE，或者如果您需要更改证书的任何部分（主题和位长度除外），则必须使用MMC方法。

1. 通过IIS管理

   使用以下步骤通过IIS管理器生成证书签名请求(CSR)。

   1. 导航到IIS Administration。
   2. 在左侧的“连接”树中选择服务器名称。
   3. 在中心窗格中找到Server Certificates，然后双击将其打开。
   4. 从右侧的Actions窗格中选择Create Certificate Request...。系统将显示Request Certificate向导。
   5. 在Distinguished Name Properties页面上，以系统的形式输入值。必须输入所有字段。选择Next继续。
   6. 在Cryptographic Service Provider Properties页上，保留Cryptographic service provider的默认选择：。将Bit length：下拉更改为最小为2048。选择Next继续。
   7. 在File Name页面上，选择要保存CSR文件的位置。
   8. 向CA提供文件。收到签名证书后，将其复制到Web服务器并继续下一步。
   9. 在IIS管理器的同一位置，在操作窗格中选择完成证书请求。系统将显示向导。
   10. 在Specify Certificate Authority Response页面上，选择CA提供的证书。在“友好名称”(Friendly name)框中指定名称。此名称是证书在下一个主要步骤的选择过程中的显示方式。确保Select a certificate store for the new certificate:下拉列表设置为Personal。
   11. 选择OK完成证书上传。
   12. 继续下一个主要步骤，将证书绑定到网站。
2. 通过Microsoft管理控制台(MMC)

   使用以下步骤通过MMC生成CSR。此方法允许您自定义CSR的每个方面。

   1. 右键单击“开始”按钮，然后选择“运行”。
   2. 在运行框中键入mmc，然后选择确定。
   3. 将证书管理单元添加到MMC窗口。
      1. 选择文件，然后选择添加/删除管理单元……系统将显示Add or Remove Snap-ins框。
      2. 在左侧列表中，找到Certificates，然后选择Add >。系统将显示Certificates管理单元框。
      3. 选择Computer account选项，然后选择Next >。
      4. 确保在选择计算机页面上选择了Local computer：（此控制台所在的计算机），然

后选择完成。
5. 选择确定以关闭添加或删除管理单元框。

4. 生成CSR
    1. 在左侧窗格中，展开证书（本地计算机），然后选择个人，然后选择证书文件夹。
    2. 右键单击Certificates文件夹并导航到All Tasks > Advanced Operations >，然后选择Create Custom Request...。系统将显示证书注册向导。
    3. 在简介屏幕中选择Next。
    4. 在Select Certificate Enrollment Policy页面上，选择Proceed without enrollment policy(在Custom Request下列出)，然后选择Next。
    5. 在Custom request页面上，确保所选Template为(No template)CNG key，并且Request format适合您的CA。PKCS #10可与Microsoft CA配合使用。选择Next以进入下一页。
    6. 在Certificate Information页面上，选择Details一词旁边的下拉列表，然后选择Properties按钮。系统将显示Certificate Properties表单。
    7. 为“证书属性”表单提供所有选项超出了本文档的范围范围。有关详细信息，请参阅Microsoft文档。以下是此表单的一些备注和提示。
        - 确保填写“主题：”选项卡的“主题名称：”部分中的所有必填值
        - 确保在Alternative name：部分中还提供了为Common name提供的值
        - 将Type:设置为DNS，在Value:框中键入URL，然后选择Add >按钮
        - 如果您希望使用多个URL访问ECE，请在此同一字段中提供每个备用名称，并在每个备用名称后选择Add >
        - 确保将Private Key选项卡上的Key size设置为大于1024的值。
        - 如果计划导出证书以便在多个Web服务器上使用（通常在HA安装中进行），请确保选择Make private key exportable。如果未能执行此操作，将导致无法在以后导出证书
        - 您输入的值和所做的选择不会被验证。您必须确保提供所有必需信息，否则CA无法完成CSR
    8. 选择所有选项后，选择OK以返回向导。选择Next以进入下一页。
    9. 在要将脱机请求保存到何处？页面上，选择您能够访问的位置中的文件名。对于大多数CA，必须选择Base 64作为格式。
    10. 将该文件提供给您的CA。当他们签名并将证书返回给您后，将证书复制到Web服务器并继续执行最后步骤。
    11. 在MMC的证书管理管理单元中，导航到证书（本地计算机）> 个人，右键单击证书，然后选择所有任务>导入……。系统将显示证书导入向导。
    12. 在介绍性屏幕上选择Next。
    13. 在File to import屏幕上，选择已由CA签名的证书，然后选择Next。
    14. 确保选择Place all certificates in the following store。
    15. 确保在证书存储：框中选择了个人，然后选择下一步。
    16. 检查最终屏幕，然后选择完成完成导入。
    17. 关闭MMC控制台。如果系统提示您保存控制台设置，请选择No。这不会影响证书导入。
    18. 继续下一个主要步骤，将证书绑定到网站。

步骤 1.2将证书绑定到网站

⚠ 注意：必须确保主机名字段留空，并且在“编辑站点绑定”框中未选择“需要服务器名称指示”选项。如果其中任何一个已配置，SPOG在尝试与ECE通信时失败。

1. 打开Internet Information Services(IIS)管理器（如果您以前未执行此操作）。
2. 在左侧的Connections窗格中，导航到Sites，然后选择Default Web Site。

   如果选择使用除“默认网站”以外的网站名称，请确保选择正确的网站名称。

3. 从右侧的操作窗格中选择Bindings..(Bindings..)。此时将显示“站点绑定”框。
    1. 如果没有Type、https和Port、443的行，请完成以下操作。否则，请继续下一个主要步骤。
        1. 选择Add...按钮，出现Add Site Binding框。
        2. 在Type:下拉列表中选择https。
        3. 确保IP address:下拉列表显示All Unassigned，且Port:字段为443。
        4. 确保将Host name：字段留空，并取消选中Require Server Name Indication选项。
        5. 在SSL certificate:下拉列表中，选择与您之前创建的证书对应的证书名称。
            - 如果您不确定要选择哪个证书，请使用选择……按钮查看和搜索服务器上存在的证书
            - 使用View...按钮查看所选证书并验证详细信息是否正确
        6. 选择OK以保存选择。
    2. 选择在“类型”列中显示https的行，然后选择编辑……按钮。系统将显示Edit Site Binding框。
        1. 确保IP address:下拉列表显示All Unassigned，且Port:字段为443。
        2. 确保将Host name：字段留空，并且未选择Require Server Name Indication选项。
        3. 在SSL certificate:下拉列表中，选择与您之前创建的证书对应的证书名称。
            - 如果您不确定要选择哪个证书，请使用选择……按钮查看和搜索服务器上存在的证书
            - 使用View...按钮查看所选证书并验证详细信息是否正确
        4. 选择OK以保存选择。
    3. 选择关闭以返回到IIS管理器。
4. 关闭IIS管理器。

第二步：配置分区管理员SSO

分区管理员SSO配置允许ECE为在SPOG中打开ECE小工具的管理员自动创建分区级别用户帐户。

✎ 注意：即使不计划启用代理或主管SSO，也必须配置分区管理员SSO。

步骤 2.1获取Active Directory(AD)证书并创建密钥库。

要解决Microsoft最近宣布的安全更改，可能需要执行此步骤。如果未应用更新且未对域进行更改，则可以跳过此步骤。

有关详细信息，请参阅Microsoft KB4520412详细信息。

1. 从您在“分区管理员配置”表单中提供的AD服务器获取Base 64格式的SSL证书。这里显示了一

种方法。

1. 使用工作站从OpenSSL下载并安装适用于Windows的OpenSSL副本。Light版已经足够了。
2. 启动OpenSSL命令提示符。
3. 运行此命令。使用全局编录域控制器的完全限定名称替换服务器名称。
   openssl s_client -connect gcdcsrv01.example.local:3269
4. 在输出中，找到服务器证书行。

```
C:openssl s_client -connect 14.10.162.6:3269
CONNECTED(00000003)
depth=1 DC = com, DC = massivedynamic, CN = MassiveDynamic Enterprise CA
verify error:num=20:unable to get local issuer certificate
verify return:0
---
Certificate chain
 0 s:
   i:/DC=com/DC=massivedynamic/CN=MassiveDynamic Enterprise CA
 1 s:/DC=com/DC=massivedynamic/CN=MassiveDynamic Enterprise CA
   i:/C=US/OU=pki.uclabservices.com/O=Cisco Systems Inc/CN=UCLAB Services Root
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIH1DCCBbygAwIBAgITJwAAAAbAAn/HKFuWCQAAAAAABjANBgkqhkiG9w0BAQsF
ADBcMRMwEQYKCZImiZPyLGQBGRYDY29tMR4wHAYKCZImiZPyLGQBGRYObWFzc2l2
ZWR5bmFtaWMxJTAjBgNVBAMTHE1hc3NpdmVEeW5hbWljIEVudGVycHJpc2UgQ0Ew
HhcNMjAwNDE1MDAxNDM0WhcNMjEwNDE1MDAxNDM0WjAAMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAxFajhqjrWqQHfqTXg+SXP5pzvNVrTHIigrAam8D0
```

5. 将输出从“BEGIN CERTIFICATE”-----“BEGIN CERTIFICATE-----”复制到“-----END CERTIFICATE-----”。确保包括BEGIN CERTIFICATE和END CERTIFICATE行。
6. 将复制的信息粘贴到新的文本文件中，然后使用crt扩展名将其保存到计算机。

2. 将证书文件复制到其中一个应用服务器。
3. 打开与复制证书的应用服务器的RDP会话。
4. 创建新的Java密钥库。
   1. 在应用服务器上打开命令提示符。
   2. 更改为ECE Java Development Kit(JDK)bin目录。
   3. 运行此命令。根据需要替换这些值。
      keytool -import -trustcacerts -alias mydomaincontroller -file C:\temp\domainctl.crt -keystore c:\ece\pcce\mydomain.jks -storepass MyP@ssword
5. 在12.6之前的版本中，将密钥库复制到环境中所有其他应用程序服务器上的同一路径。使用版本12.6，将密钥库复制到您配置ECE的工作站可访问的位置。

步骤 2.2使用AD轻型目录访问协议(LDAP)访问信息配置ECE。

1. 从使用Internet Explorer 11的工作站或计算机，导航到业务分区URL。

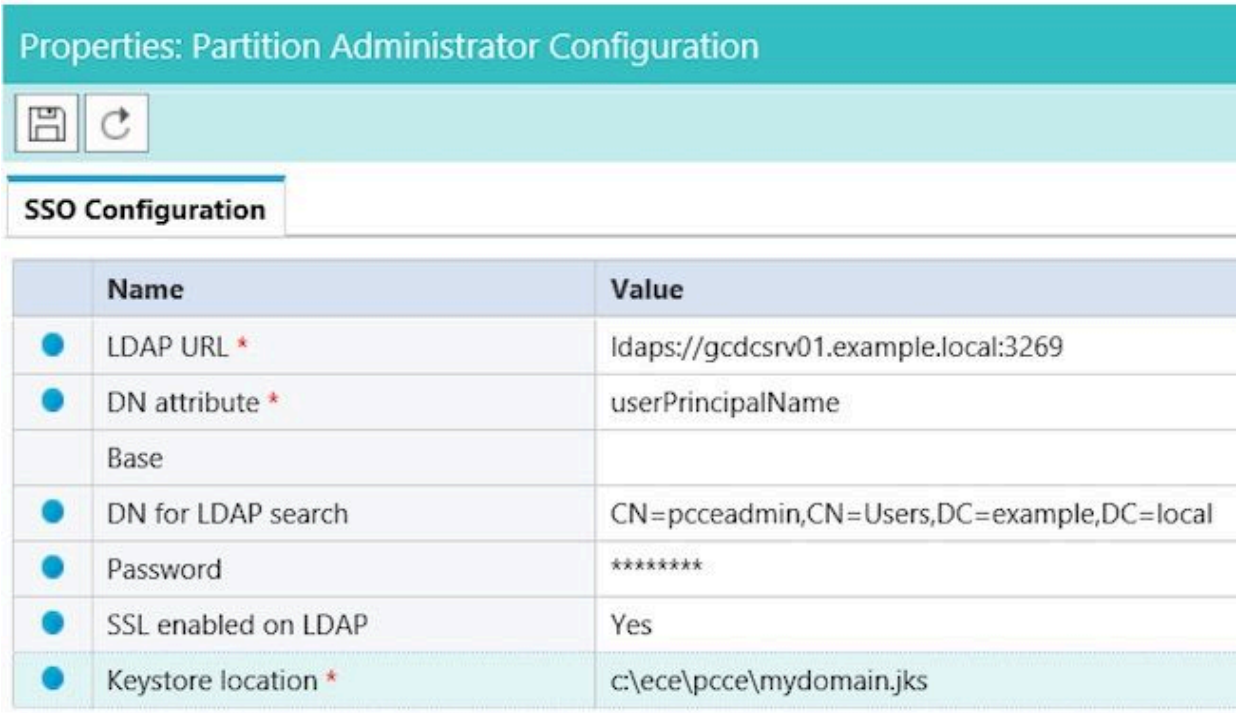
> 提示：业务分区也称为分区1。对于大多数安装，可以通过类似https://ece.example.com/default的URL访问业务分区。

2. 以pa身份登录，并提供系统的密码。
3. 成功登录后，在初始控制台上选择Administration链接。

4. 导航到SSO Configuration文件夹，Administration > Partition: default > Security > SSO and Provisioning。
5. 在右侧的顶部窗格中，选择Partition Administration Configuration条目。
6. 在右侧底部窗格中，输入轻量级目录访问协议(LDAP)和AD的值。
    1. LDAP URL — 作为一种最佳实践，请使用全局目录(GC)域控制器的名称。
       如果不使用GC，则在ApplicationServer日志中会看到错误，如下所示。
       LDAP身份验证时出现异常<@>
       javax.naming.PartialResultException：未处理的继续引用；剩余名称
       “DC=example，DC=com”
        - 非安全全局目录端口为3268
        - 安全全局目录端口为3269
    2. DN属性 — 必须为userPrincipalName。
    3. Base — 如果使用GC，则不需要此项，否则，必须提供基本正确的LDAP格式。
    4. LDAP搜索的DN — 除非您的域允许匿名绑定，否则您必须提供能够绑定到LDAP并搜索目录树的用户的可分辨名称。

       提示：为用户找到正确值的最简单方法是使用Active Directory用户和计算机工具。这些步骤显示如何查找此值。

        1. 从View菜单中，选择Advanced Features选项。
        2. 导航到用户对象，然后右键单击并选择属性。
        3. 选择Attributes选项卡。
        4. 选择Filter按钮，然后选择Only show attributes with values。
        5. 在列表中查找distinquishedName，然后双击以查看值。
        6. 突出显示显示的值，然后将其复制并粘贴到文本编辑器。
        7. 将文本文件中的值复制并粘贴到DN for LDAP搜索字段中。
           该值必须类似于CN=pcceadmin、CN=Users、DC=example、DC=local
    5. Password — 提供指定用户的密码。
    6. 在LDAP上启用SSL — 此字段对于大多数客户来说可能是必需的。
    7. 密钥库位置 — 这必须是从AD导入SSL证书的密钥库位置。在本示例中，这是c:\ece\pcce\mydomain.jks，如图所示：



7. 选择软盘的图标以保存更改。

第三步：验证配置文件

对于所有12.0安装，必须完成本部分。对于12.0以外的任何版本，可以跳过此部分。
对于所有版本，可能还需要执行此步骤的两个其他场景。第一种是将ECE安装在高可用性设置中时。第二种（也是更常见的）是Web服务器的主机名与用于访问ECE的名称不匹配。例如，如果将ECE Web服务器安装在主机名为UCSVRECEWEB.example.com的服务器上，但用户使用URL chat.example.com访问ECE网页，则必须完成此部分。如果服务器主机名和使用访问ECE的URL相同，并且安装了版本12.5或更高版本，则可以跳过此步骤并完成此部分。

将{ECE_HOME}替换为安装了ECE的物理位置。例如，如果已在C:\Cisco安装ECE，则在每个位置将{ECE_HOME}替换为C:\Cisco。

提示：使用记事本++等文本编辑器，而不是记事本或写字板，因为这些文本编辑器无法正确解释行尾。

---

1. 打开与部署中的所有ECE Web服务器的远程桌面会话。
2. 导航到此路径:{ECE_HOME}\eService\templates\finesse\gadget\spog。
3. 找到spog_config.jsfile，并在安全位置创建备份副本。
4. 在文本编辑器中打开当前spog_config.jsfile。
5. 找到这两行并更新它们以匹配您的部署。
   web_server_protocol必须是https，如有必要，请更新。
   更新web_server_name以匹配您分配用于访问ECE的完全限定名称。示例：ece.example.com
   - var web_server_protocol = "https";
   - var web_server_name = "ece.example.com";
6. 保存更改。
7. 在部署中的所有其他Web服务器上重复上述步骤。

第四步：将ECE添加到PCCE库存

截至12.0,PCCE有3个不同的部署选项：2000代理（2K代理）、4000代理（4K代理）和12000代理（12K代理）。这三个部署选项可分为两组：2K Agent和4K/12K Agent。它们以这种方式分离，因为它们在SPOG中的外观存在一些根本性的差异。本段对这两种方法作了非常详细的比较。本文档不提供将组件添加到库存的具体步骤。请参阅本文档末尾的链接，了解此流程的具体详细信息。本节介绍将ECE添加到PCCE时必须验证的特定详细信息。本文档还假定您的PCCE安装已完成，并且您能够访问和配置解决方案的其他方面。

- 2K代理部署
  - PCCE组件的初始配置完全通过CCE管理完成，并且是自动的
  - 新组件通过弹出框添加到资产页面，您可以在其中输入详细信息（如IP或主机名以及任何必要的凭证或特定于组件的配置）
- 4K和12K代理部署
  - 大部分初始配置都反映了用于UCCE的步骤
  - 组件通过从CCE管理下载的逗号分隔值(CSV)文件添加，根据特定安装进行填充，然后上传
  - 初始部署要求在第一个CSV文件中包含某些特定组件
  - 最初设置系统时未添加的组件通过包含所需信息的CSV文件添加

步骤 4.1将ECE Web服务器证书上传到Java密钥库

1. 如果使用自签名证书
   1. 打开与主A端管理数据服务器(ADS)的远程桌面连接。
   2. 以管理员身份打开Internet Explorer 11并导航到ECE业务分区。
   3. 选择URL栏右侧的挂锁图标，然后选择View Certificates。
   4. 在Certificate框中，选择Details选项卡。
   5. 选择靠近选项卡底部的Copy to File..。
   6. 在Certificate Export Wizard中，选择Next，直到您到达Export File Format页。确保选择Base-64编码的X.509(.CER)格式。
   7. 将证书保存到ADS服务器上的c:\Temp\certificates等位置，以完成导出。
   8. 将证书复制到所有其他ADS服务器。
   9. 打开管理命令提示符。
   10. 切换到Java主目录，然后切换到bin目录。Java主目录可通过以下方式访问。cd %JAVA_HOME%\bin
   11. 备份当前的cacerts文件。将cacerts文件从%JAVA_HOME%\lib\security复制到其他位置。
   12. 运行此命令以导入之前保存的证书。如果您的密钥库密码不是“changeit”，请更新命令以匹配您的安装。
       keytool -keystore ../lib/security/cacerts -storepass changeit -import -alias <ECE服务器的FQDN> -file <保存证书的位置>
   13. 重新启动ADS服务器。
   14. 在其他ADS服务器上重复步骤8-12。
2. 如果使用CA签名的证书
   1. 获取DER/PEM格式的根证书和中间证书，并将它们复制到所有ADS服务器上C:\Temp\certificates等位置。

注意：请与您的CA管理员联系以获取这些证书。

2. 打开与主A侧ADS的远程桌面连接。
3. 打开管理命令提示符。
4. 切换到Java主目录，然后切换到bin目录。Java主目录可通过以下方式访问。cd %JAVA_HOME%\bin
5. 备份当前的cacerts文件。将cacerts文件从%JAVA_HOME%\lib\security复制到其他位置。
6. 运行此命令以导入之前保存的证书。如果您的密钥库密码不是“changeit”，请更新命令以匹配您的安装。
   keytool -keystore ../lib/security/cacerts -storepass changeit -trustcacerts -import -alias <CA根的名称> -file <保存根证书的位置>
7. 重复步骤6.并导入中间证书（如果有）。
8. 重新启动ADS服务器。
9. 在所有其他ADS服务器上重复步骤2-12。

步骤 4.2将ECE数据服务器添加到库存

- 当数据服务器必须存在于系统清单中时，PCCE ADS和数据服务器之间不会进行直接通信
- 在1500代理部署中部署ECE时，数据服务器是服务服务器
- 当ECE安装在HA配置中时，仅添加A端服务服务器

步骤 4.3将ECE Web服务器添加到库存

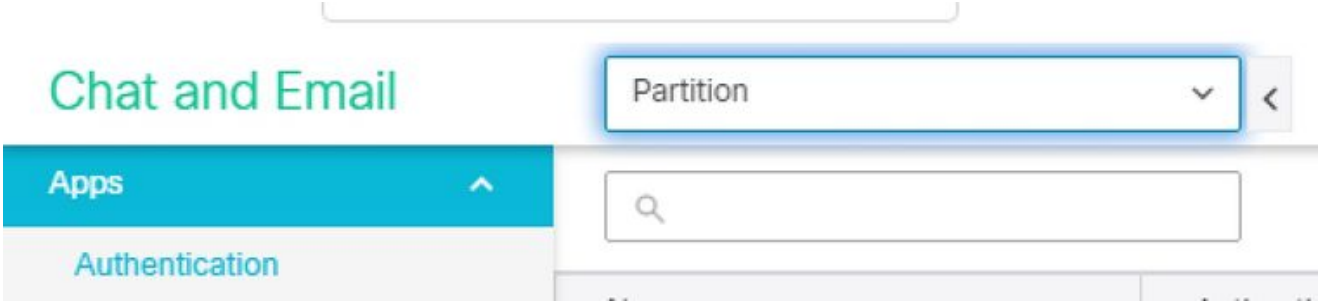
- 确保使用完全限定名称添加Web服务器
  - 此名称必须与ECE证书中的公用名称匹配，或者必须列为主题备用名称(SAN)之一
  - 不能仅使用主机名或IP地址
- ECE的用户名和密码必须是pa登录凭证
- 确保应用程序实例正确
  - 应用程序实例名称区分大小写
  - 对于2000座席PCCE部署，应用实例为MultiChannel
  - 对于4000/12000座席PCCE部署，应用实例包含站点和外设集作为名称的一部分
- 当ECE安装有多个Web服务器时，例如，在1500代理部署或400代理HA部署中，您可以使用指向负载均衡器的URL或指向每个Web服务器的URL作为Web服务器的完全限定名称。最佳实践是使用负载均衡器。
- 如果您有多个ECE部署，或者如果您选择在部署中添加多个单独的Web服务器，则在SPOG中打开ECE小工具时，您会选择正确的Web服务器。

第五步：将ECE与PCCE集成

1. 以管理员身份登录到CCE管理。
2. 选择Email and Chat卡，然后选择Email and Chat链接（如图所示）。



3. 在Device Name下拉列表中查看当前选定的服务器。如果在HA安装中添加了两个Web服务器，则可以选择其中一个Web服务器。如果稍后向系统中添加第二个ECE部署，请确保选择适当的服务器，然后再继续。
4. 在Chat and Email旁边的下拉列表中，选择Partition或Global，如图所示。



5. 在顶部菜单中，选择Integration，然后选择Unified CCE旁边的箭头并选择第二个Unified CCE，如图所示。



6. 填写安装时的AWDB Details选项卡中的值，然后选择Save按钮。
7. 选择Configuration选项卡，然后按如下方式完成此操作。
    1. 选择Application Instance旁边的下拉列表，并选择为ECE创建的应用实例。

> 注：这不能是以UQ开头的应用实例。



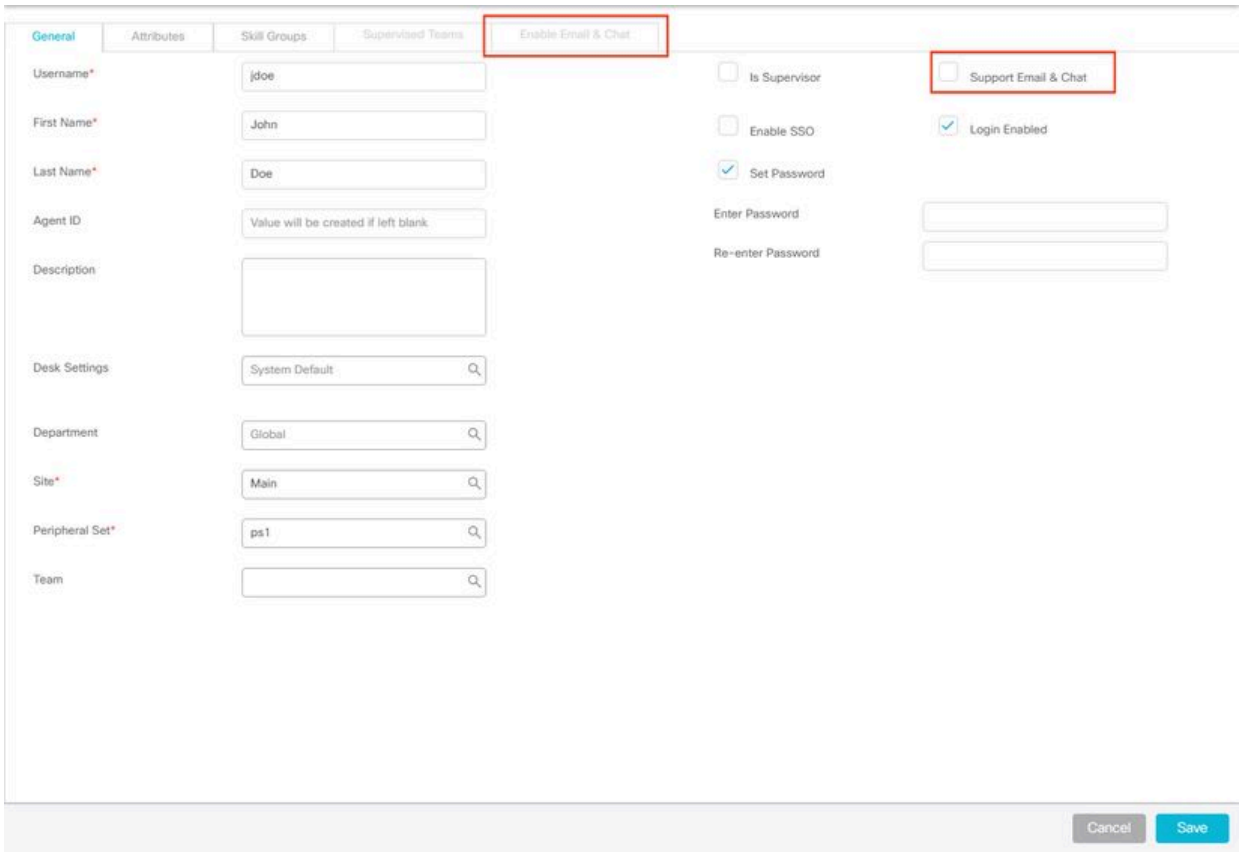
    2. 选择带白色加号的绿色圆圈按钮，选择“座席PG”。
        1. 选择“座席PG”（或者“座席PG”，如果不止一个）。
        2. 添加所有座席PG后，请选择Save。

> 警告：选择Save后，系统已永久连接到PCCE，且无法撤消。如果本节中出错，则必须完全卸载ECE并删除所有数据库，然后像全新安装一样安装ECE。

第六步：验证ECE集成

1. 在“CCE管理”中，检查顶部状态栏中是否未显示警报。 如果有警报，请选择警报一词并查看“清单”页面，以确保没有任何警报适用于ECE服务器。
2. 在左侧导航栏中选择Users，然后选择Agents。

3. 从列表中选择一个座席并检验它。
    1. 您现在会在General选项卡上看到Support Email & Chat的新复选框。
    2. 现在，您会看到一个标记为Enable Email & Chat的新选项卡，如图所示。



4. 启用ECE测试代理。
    1. 选中Support Email & Chat复选框，并注意Enable Email & Chat选项卡现在可选中。
    2. 选择Enable Email & Chat选项卡，并在Screen Name字段中提供值。
    3. 选择Save以更新用户。
    4. 您会收到成功消息。
5. 确认ECE已更新。
    1. 选择Overview导航按钮，然后选择Email and Chat卡和链接。
    2. 在Chat and Email旁边的下拉列表中，选择与座席部门对应的名称。

> 注：ECE中的服务部门保存属于PCCE中的全局部门的所有对象。因此，部门名称Service是保留值。

        1. 在顶部菜单中，选择User Management，然后在Chat and Email下的菜单中选择Users。
        2. 验证您是否在列表中看到新座席。

故障排除

建议您下载多个工具并将其保存在ECE服务器上。这样可以更轻松地排除故障并随着时间的推移维护解决方案。

- 文本编辑器，如记事本++

- 存档工具，如7-Zip
- Windows程序的众多Tail之一
  下面是一些示例：
  - Baretail
  - Win32的尾部

为了排除集成问题，您必须首先了解一些关键日志文件和每个日志文件的位置。

1. ECE上的文件名和位置

   ECE系统上有许多日志，这些日志在您尝试解决集成问题时非常有帮助。

日志文件	服务器	名称约定	描述
应用服务器	客户经理	eg_log_{HOSTNAME}_ApplicationServer.log	来自Wildfly服务器的日志
外部座席分配	呼叫/秒	eg_log_{HOSTNAME}_EAAS-process.log	与MR PG互动
外部代理消息传送	呼叫/秒	eg_log_{HOSTNAME}_EAMS-process.log	与CTI服务器的交互
根日志	C/A/M/S	egpl_root_{HOSTNAME}.log	进程间日志、HazelCast、常规错误
组件状态	C/A/M/S	eg_log_{HOSTNAME}_component-status.log	进程开始和文件复制完成
进程启动器	C/A/M/S	eg_log_{HOSTNAME}_ProcessLauncher.log	服务和进程启动的一般日志
分布式服务管理器	呼叫/秒	eg_log_{HOSTNAME}_DSMController.log	显示进程在Services服务器上启动和停止的日志

   服务器密钥：

   - C =并置服务器
   - A =应用服务器
   - S =服务服务器
   - M =邮件服务器

   大多数日志文件还有另外两个与其关联的日志。

   - eg_log_{SERVERNAME}_{PROCESS}.log — 主进程日志
   - eg_log_dal_connpool_{SERVERNAME}_{PROCESS}.log — 连接池使用情况

- eg_log_query_timeout_{SERVERNAME}_{PROCESS}.log — 查询因超时而失败时更新

2. PCCE上的文件名和位置

有关集成问题的PCCE日志全部位于A侧ADS。以下是排除集成故障时最重要的日志。这些产品均位于C:\icm\tomcat\logs。

日志文件	名称约定	描述
CCBU	CCBU.{YYYY}-{MM}-{DD}T{hh}-{mm}-{ss}.{msec}.startup.log	CCE Admin和所有相关Web应用的主日志
CCBU错误	错误。{YYYY}-{MM}-{DD}T{hh}-{mm}-{ss}.{msec}.startup.log	CCE管理员和相关网络应用程序看到的错误
卡塔利纳	catalina.{YYYY}-{MM}-{DD}.log	Tomcat本机日志，显示证书错误
Tomcat stdout	tomcat9-stdout.{YYYY}-{MM}-{DD}.log	来自Tomcat的标准输出日志消息
Tomcat stderr	tomcat9-stderr.{YYYY}-{MM}-{DD}.log	来自Tomcat的标准错误日志消息

在这些日志中，前三个日志是请求和审核最频繁的。

使用这些步骤设置跟踪级别并收集所需的日志。

3. 跟踪级别配置

本节仅适用于ECE。PCCE所需的日志由思科设置其跟踪级别，并且无法更改。

1. 从使用Internet Explorer 11的工作站或计算机，导航到系统分区URL。

   提示：系统分区也称为分区0。对于大多数安装，可以通过类似https://ece.example.com/system的URL访问系统分区

2. 以sa身份登录并提供系统的密码。
3. 成功登录后，在初始控制台上选择System链接。
4. 在System页面，展开System > Shared Resources > Logger > Processes。
5. 在顶部右侧窗格中，找到要更改跟踪级别的进程并选择它。
   注意：在HA系统和具有多个应用服务器的系统中，进程会多次列出。为确保捕获数据，请为包含进程的所有服务器设置跟踪级别。
6. 在右下方的窗格中，选择Maximum trace level下拉列表并选择适当的值。
   ECE中定义了8个跟踪级别。本列表中的4个是最常用的。
   - 2 — 错误 — 进程的默认跟踪级别

- 4 — 信息 — 通常用于解决问题的跟踪级别
- 6 - Dbquery — 通常有助于在设置早期诊断问题或更复杂的问题
- 7 — 调试 — 非常详细的输出，仅在最复杂的问题中需要

注意：请勿将任何流程保留为6 - Dbquery或更高的任何时间长度，通常只在TAC指导下进行。

保持大多数进程跟踪级别，2 — 错误。如果选择级别7或8，还必须选择最长持续时间。当达到最大持续时间时间时，跟踪级别将返回到上一个级别集。
设置系统后，将这四个进程更改为跟踪级别4。

- EAAS流程
- EAMS流程
- DX进程
- rx-process

7. 选择保存图标以设置新的跟踪级别。

4. 日志文件收集

1. 打开与需要进程日志的服务器的远程桌面会话。
2. 导航到日志文件位置。
    1. ECE服务器

    日志按如下方式编写。

    - 默认情况下，日志是最大大小为5MB的已写入文件
    - 当一个日志文件达到配置的最大值时，会以{LOGNAME}.log.{#}格式重命名该日志文件
    - ECE保留以前的49个日志文件加上当前文件
    - 当前日志始终以.log结尾，并且后面没有数字
    - 日志既不存档也不压缩
    - 大多数日志具有通用结构
    - 日志文件使用<@>分隔各个部分
    - 日志始终以GMT+0000时间写入

    根据具体安装，ECE日志位于不同位置。

    1. 400代理部署
        1. 单面
            - 服务器：并置服务器
            - 位置:{ECE_HOME}\eService_RT\logs
        2. 高可用性
            - 服务器：两台并置的服务器
            - 位置:{ECE_HOME}\eService\logs
            - 为分布式文件系统(DFS)共享创建的目录仅包含用于安装和升级的日志。

- 只有拥有分布式系统管理器(DSM)角色的服务器才写入属于服务角色的组件的日志
    - 可以在Windows任务管理器的“进程”选项卡上找到DSM角色所有者。此服务器上有10-15个Java进程不在辅助服务器上。
    - DSM下的组件包括EAAS、EAMS、Retriever、Dispatcher、Workflow等。

2. 1500代理部署
    - 位于托管角色的服务器上的日志
    - 位置:{ECE_HOME}\eService\logs
    - 除服务服务器外，所有服务器都运行并写入与组件相关的所有进程的日志
    - 在高可用性部署中，服务服务器以主用/备用配置运行
    - 只有拥有分布式系统管理器(DSM)角色的服务器才能写入日志
    - DSM角色所有者可以通过Windows任务管理器中看到的进程数来确定。有10-15个Java进程在主服务器上运行，只有4个Java进程在辅助服务器上运行

2. PCCE服务器
    - PCCE所需的日志位于：C:\icm\tomcat\logs
    - Tomcat日志不会被回滚或存档
    - 日志以本地服务器时间写入

3. 收集发现问题后创建或修改的所有日志。
有关日志和所发现问题的完整说明不属于本文档的讨论范围。下面是一些常见问题、要检查的内容以及一些可能的解决方案。
    - 证书相关问题
        - 未导入证书
            - 行为：当您尝试在SPOG中打开ECE小工具时，您会看到错误“加载页面时出错。请与管理员联系。"
            - 检查：Catalina在PCCE上记录类似以下错误 javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException：无法找到指向请求目标的有效证书路径
            - 解决方案：确保您已将ECE Web服务器证书或相应的CA证书导入到ADS上的密钥库中
        - 证书不匹配
            - 行为：当您尝试在SPOG中打开ECE小工具时，您会看到一个错误，表明证书的公用名或使用者备用名与配置的名称不匹配。
            - 检查：验证SSL证书
            - 解析：确保主题中的“公用名”字段或主题替代名称中的DNS字段之一包含您在SPOG中输入的完全限定名称作为Web服务器名称。
    - 系统问题
        - 服务未启动
            - 行为：当您尝试在SPOG中打开ECE小工具时，您会看到错误：“https://{url}处的网页可能暂时关闭或永久移动到新地址。”
            - 检查：验证所有ECE服务器（Web服务器除外）上是否已启动

Windows服务 — Cisco服务。查看应用服务器上的根日志是否有错误
    - 解决方案：启动所有ECE服务的思科服务。
- 配置问题
    - LDAP配置
        - 行为：当您尝试在SPOG中打开ECE小工具时，您会看到错误“加载页面时出错。请与管理员联系。"
        - 检查：将应用服务器的跟踪级别提高到级别7 - Debug，然后再次尝试登录并查看应用服务器日志。搜索LDAP一词。
        - 解决方法：验证分区管理员SSO的LDAP配置，以确保其正确。

相关信息

这些是您在开始安装或集成任何ECE之前必须仔细阅读的重要文档。这不是一份全面的欧洲经委会文件清单。

⚠ 注意：大多数欧洲经委会文件有两个版本。请确保下载并使用适用于PCCE的版本。文档标题在版本号之后为Packaged Contact Center Enterprise或（对于PCCE）或（对于UCCE和PCCE）。

确保您在安装、升级或集成之前查看思科企业聊天和电子邮件文档的起始页面以获取任何更新。

https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/series.html

- 12.0
    - 企业聊天和电子邮件安装和配置指南
    - 企业聊天和电子邮件升级指南
    - 企业聊天和电子邮件管理员指南
- 12.5
    - 企业聊天和电子邮件安装和配置指南
    - 企业聊天和电子邮件升级指南
    - 企业聊天和电子邮件管理员指南

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。