证书

数字证书是一种用于身份验证的数字识别方式。证书用于 SSL（安全套接字层）、TLS（传输层安全）和 DTLS（数据报 TLS）连接，例如 HTTPS 和 LDAPS。以下主题介绍如何创建和管理证书。

关于证书

数字证书是一种用于身份验证的数字识别方式。数字证书包括用于识别设备或用户的信息，例如名称、序列号、公司、部门或 IP 地址。数字证书还包括用户或设备的公钥副本。证书用于 SSL（安全套接字层）、TLS（传输层安全）和 DTLS（数据报 TLS）连接，例如 HTTPS 和 LDAPS。

您可以创建以下类型的证书：

- 内部证书 - 内部身份证书是用于特定系统或主机的证书。您可以使用 OpenSSL 工具包自己生成这些证书，也可以从证书颁发机构获取这些证书。此外，您还可以生成自签名证书。当内部证书因任何原因到期或无效时，您可以通过以下 CLISH CLI 命令重新生成证书：

  ```
  > system support regenerate-security-keyring
    String  Certificate to be regenerated, default or fdm
  ```

- 内部证书颁发机构 (CA) 证书 - 内部 CA 证书是系统可用于签署其他证书的证书。这些证书与内部身份证书的区别在于基本限制条件扩展和 CA 标记方面，CA 证书启用了这些功能，而身份证书中则禁用了这些功能。您可以使用 OpenSSL 工具包自己生成这些证书，也可以从证书颁发机构获取这些证书。此外，您还可以生成自签名的内部 CA 证书。如果配置自签名的内部 CA 证书，该 CA 将在设备自身上运行。

- 可信证书颁发机构 (CA) 证书 - 可信的 CA 证书可用于签署其他证书。它是自签名证书，也称为根证书。由另一个 CA 证书颁发的证书称为从属证书。

证书颁发机构 (CA) 是指“签署”证书以确认其真实性，从而确保设备或用户的身份的可信颁发机构。CA 在 PKI（使用公钥或私钥加密以确保安全性）的情景下颁发数字证书。CA 可以是可信的第三方（例如 VeriSign），也可以是组织内建立的私有（内部）CA。CA 负责管理证书请求和颁发数字证书。有关详细信息，请参阅公钥加密，第 2 页。

公钥加密

在 RSA 加密系统等公钥加密中，每位用户都有一个包含公钥和私钥的密钥对。这一对密钥相互补充，用其中一个密钥加密的任何内容都可用另一个密钥解密。

简言之，使用私钥加密数据时会形成一个签名。此签名附加在数据中并发送给接收者。接收者对数据应用发送者的公钥。如果随数据一起发送的签名与对数据应用公钥的结果一致，就会确立消息的有效性。

此过程的前提是接收者拥有发送者的公钥副本而且非常确定此密钥属于发送者，而不是伪装成发送者的其他人。

获取发送方公钥通常是在外部处理或通过安装时执行的操作处理。例如，默认情况下，大多数 Web 浏览器都使用若干 CA 的根证书进行配置。

您可以通过 openssl.org、维基百科或其他来源了解有关数字证书和公钥加密的更多信息。充分了解 SSL/TLS 加密有助于您为自己的设备建立安全连接。

功能使用的证书类型

您需要为每个功能创建正确类型的证书。以下功能需要证书。

身份策略（强制网络门户）- 内部证书

（可选。）强制网络门户用于身份策略中。在向设备进行身份验证时，为了标识自己的身份并获得与其用户名关联的 IP 地址，用户必须接受此证书。如果不提供证书，设备将使用自动生成的证书。

身份领域（身份策略和远程访问 VPN）- 受信任的 CA 证书

（可选。）如果对目录服务器进行加密连接，则必须接受证书才能在目录服务器上执行身份验证。当系统按身份和远程访问 VPN 策略提示用户进行身份验证时，用户必须进行身份验证。如果不对目录服务器使用加密，则不需要证书。

管理 Web 服务器（管理访问系统设置）- 内部证书

（可选） 设备管理器 是基于 Web 的应用，所以在 Web 服务器上运行。您可以上传您的浏览器视为有效的证书，以避免出现“不受信任的颁发机构”警告。

远程访问 VPN - 内部证书

（必需。）内部证书用于外部接口，在 Secure Client 与设备进行连接时确定客户端的设备身份。客户端必须接受此证书。

站点间 VPN - 内部和受信任 CA 证书

如果对站点间 VPN 连接使用证书身份验证，您需要选择用于对连接中的本地对等体进行身份验证的内部身份证书。虽然这并不是 VPN 连接定义的一部分，但您还需要上传用于签署本地和远程对等体身份证书的受信任 CA 证书，以便系统可以对对等体进行身份验证。

SSL 解密策略 - 内部、内部 CA 和受信任 CA 证书以及证书组

（必需。）SSL 解密策略将证书用于以下目的：

- 内部证书用于已知的密钥解密规则。
- 在客户端和 威胁防御 设备之间创建会话时，内部 CA 证书用于解密重签名规则。
- 在 威胁防御 设备和服务器之间创建会话时，受信任 CA 证书直接用于解密重签名规则。受信任 CA 证书用于验证服务器证书的签名机构。您可以直接配置这些证书或在策略设置的证书组中进行配置。系统包括大量受信任 CA 证书（集中放置于 Cisco-Trusted-Authorities 组中），因此您可能无需上传任何其他证书。

示例：使用 OpenSSL 生成内部证书

以下示例使用 OpenSSL 命令生成内部服务器证书。您可以从 openssl.org 获取 OpenSSL。有关具体信息，请查阅 OpenSSL 文档。此示例中使用的命令可能会更改，您还可以使用其他您可能想要使用的可用选项。

此程序旨在让您了解如何获取要上传到 威胁防御 的证书。

注释 这里显示的 OpenSSL 命令仅作为示例。调整参数以满足您的安全要求。

过程

步骤 1 生成密钥。

```
openssl genrsa -out server.key 4096
```

步骤 2 生成证书签名请求 (CSR)。

```
openssl req -new -key server.key -out server.csr
```

步骤 3 使用密钥和 CSR 生成自签证书。

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

由于 设备管理器 不支持加密的密钥，请尝试在生成自签证书时按回车键跳过质询密码。

步骤 4 在 设备管理器中创建内部证书对象时，将文件上传到相应的字段。

您还可以复制/粘贴文件内容。示例命令创建以下文件：

- server.crt - 将内容上传或粘贴到“服务器证书”字段中。
- server.key - 将内容上传或粘贴到“证书密钥”字段中。如果您在生成密钥时提供了密码，则可以使用以下命令对其进行解密。输出发送到 stdout，您可以从其中复制它。

```
openssl rsa -in server.key -check
```

配置证书

威胁防御 支持 PEM 或 DER 格式的 X509 证书。如果需要，可使用 OpenSSL 生成证书、从受信任的证书颁发机构获取证书或创建自签名证书。

有关证书的详细信息，请参阅关于证书，第 1 页。

有关每项功能所用证书类型的信息，请参阅功能使用的证书类型，第 2 页。

以下步骤程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。此外，也可以在编辑证书属性时，点击对象列表中所示的**创建新证书**链接来创建证书对象。

过程

步骤 1 选择**对象**，然后从目录中选择**证书**。

系统提供以下预定义证书（您可以按原样使用或替换它们）。

- DefaultInternalCertificate
- DefaultWebserverCertificate
- NGFW-Default-InternalCA

此外，系统还包括许多从第三方证书颁发机构获取的受信任的 CA 证书。SSL 解密策略可使用这些证书执行解密重新签署操作。Cisco-Trusted-Authorities 组包括所有这些证书，并且是 SSL 解密策略使用的默认组。

可以点击预定义的搜索过滤器，将列表限制为仅**系统定义**或**用户定义**的证书。您还可以使用**弱密钥**过滤器来查找密钥短于建议最小长度的证书。建议您将这些证书替换为具有更长密钥的证书。

步骤 2 执行以下操作之一：

- 要创建新的证书对象，请使用 + 菜单中适合证书类型的命令。
- 要创建新证书组，请点击 并选择**添加证书组**。
- 要查看或编辑证书或组，请点击证书的编辑图标 () 或查看图标 ()。
- 要删除未引用的证书或组，请点击证书的垃圾桶图标 ()。

有关创建或编辑证书的详细信息，请参阅下列主题：

- 上传内部证书和内部 CA 证书，第 5 页

- 生成自签名的内部证书和内部 CA 证书，第 6 页
- 上传受信任的 CA 证书，第 8 页
- 配置受信任 CA 证书组，第 9 页

上传内部证书和内部 CA 证书

内部身份证书是特定系统或主机的证书。

内部 CA 证书是系统可用于签署其他证书的证书。这些证书与内部身份证书的区别在于基本限制条件扩展和 CA 标记方面，CA 证书启用了这些功能，而身份证书中则禁用了这些功能。

您可以使用 OpenSSL 工具包自行生成这些证书，也可以从证书颁发机构获取证书，然后再按照以下步骤程序上传证书。有关生成密钥的示例，请参阅示例：使用 OpenSSL 生成内部证书，第 3 页。

此外，您还可以生成自签名的内部身份和内部 CA 证书。如果配置自签名的内部 CA 证书，该 CA 将在设备自身上运行。有关创建自签名证书的信息，请参阅生成自签名的内部证书和内部 CA 证书，第 6 页。

有关使用这些证书的功能的信息，请参阅功能使用的证书类型，第 2 页。

过程

步骤 1 选择**对象**，然后从目录中选择**证书**。

步骤 2 执行以下操作之一：

- 依次点击 + > **添加内部证书**，然后点击**上传证书和密钥**。
- 依次点击 + > **添加内部 CA 证书**，然后点击**上传证书和密钥**。
- 要编辑或查看证书，请点击信息图标( )。对话框中将显示证书主题、颁发者和有效时间范围。点击“替换证书”即可上传新的证书和密钥。此外，您还可以在对话框中粘贴证书和密钥。

步骤 3 键入证书的**名称**。

该名称仅在配置中用作对象名称，不会成为证书本身的一部分。

步骤 4 点击**上传证书**（或在编辑时点击**替换证书**），并选择证书文件（例如 *.crt）。允许的文件扩展名有 .pem、.cert、.cer、.crt 和 .der。或者，粘贴证书。

该证书必须为 PEM 或 DER 格式的 X509 证书。

您粘贴的证书必须包括 BEGIN CERTIFICATE 和 END CERTIFICATE 行。例如：

```
-----BEGIN CERTIFICATE-----
MIICMTCCAZoCCQDdUV3NGK/cUjANBgkqhkiG9w0BAQsFADBdMQswCQYDVQQGEwJV
UzETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50ZXJuZXQgV2lkZ2l0
(...5 lines removed...)
```

```
shGJDReRYJQqilhHZrYTWZAYTrD7NQPHutK+ZiJng67cPgnNDuXEn55UwMOQoHBp
HMUwmhiGZlzJM8BpX2Js2yQ3ms30pr8rO+gPCPMCAwEAATANBgkqhkiG9w0BAQsF
AAOBgQCB02CebA6YjJCGr2CJZrQSeUwSveRBpmOuoqm98o2Z+5gJM5CkqgfxwCUn
RV7LRfQGFYd76V/5uor4Wx2ZCjqy6+zuQEm4ZxWNSZpA9UBixFXJCs9MBO4qkG5D
vlk3WYJfcgyJ10h4E4b0W2xiixBU+xoOTLRATnbKY36EWAG5cw==
-----END CERTIFICATE-----
```

步骤 5 点击**上传密钥**（或在编辑时点击**替换密钥**），并选择证书文件（例如 *.key）。文件扩展名必须为.key。或者，粘贴证书的密钥。

该密钥无法加密，且必须是 RSA 密钥。

例如：

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQClSu1BknrMjzw/5FZ9YgdMLDUGJlbYgkjN7mVrkjyLQx2TYsem
r8iTiKB6iyTKbuS4iPeyEYkNF5FglCqKWEdmthNZkBhOsPs1A8e60r5mImeDrtw+
Cc0O5cSfnlTAw5CgcGkcxTCaGIZmXMkzwGlfYmzbJDeazfSmvys76A8I8wIDAQAB
AoGAUVDgEX8vXE0m9cOubPZ54pZo64KW/OJzUKP0TwxdLqGw/h39XFpkEXiIgmDL
(...5 lines removed...)
DSWvzekRDH83dmP66+MIbWePhbhty+D1OxbiuVuHV0/ZhxOhCG8tig3R8QJBAJmj
fId05+1dNI4tGbWv6hHh/H/dTP2STlZ3jERMZd29fjIRuJ9jpFC2lIDjvs8YGeAe
0YHkfSOULJn8/jOCf6kCQQDIJiHfGF/31Dk/8/5MGrg+3zau6oKXiuv6db8Rh+7l
MUOx09tvbBUy9REJq1YJWTKpeKD+E0QL+FX0bqvz4tHA
-----END RSA PRIVATE KEY-----
```

步骤 6 点击**确定 (OK)**。

如果密钥大小小于生成的自签名证书所允许的最小大小，则系统会警告您该证书不符合建议的最低要求。点击**继续**可继续上传证书，但建议您创建更强的新证书。

生成自签名的内部证书和内部 CA 证书

内部身份证书是特定系统或主机的证书。

内部 CA 证书是系统可用于签署其他证书的证书。这些证书与内部身份证书的区别在于基本限制条件扩展和 CA 标记方面，CA 证书启用了这些功能，而身份证书中则禁用了这些功能。

您可以生成自签名的内部身份和内部 CA 证书，即这些证书由设备自身签署。如果配置自签名的内部 CA 证书，该 CA 将在设备上运行。系统会生成证书和密钥。

此外，还可以使用 OpenSSL 创建证书或从受信任的 CA 获取证书，再上传它们。有关详细信息，请参阅上传内部证书和内部 CA 证书，第 5 页。

有关使用这些证书的功能的信息，请参阅功能使用的证书类型，第 2 页。

过程

步骤 1 选择**对象**，然后从目录中选择**证书**。

步骤 2 执行以下操作之一：

- 依次点击 + > **添加内部证书**，然后点击**自签名证书**。
- 依次点击 + > **添加内部 CA 证书**，然后点击**自签名证书**。

注释 要编辑或查看证书，请点击信息图标 ( )。对话框中将显示证书主题、颁发者和有效时间范围。点击**替换证书**，可上传新的证书和密钥。替换证书后，不能重新执行以下步骤中介绍的自签名特性设置。相反，您必须粘贴或上传新的证书，如上传内部证书和内部 CA 证书，第 5 页中所述。其余步骤仅适用于新的自签名证书。

步骤 3 键入证书的**名称**。

该名称仅在配置中用作对象名称，不会成为证书本身的一部分。

步骤 4 为证书主题和颁发者信息至少配置以下一项。

- **国家/地区** (C) - 证书中包括的双字符 ISO 3166 国家/地区代码。例如，美国的国家/地区代码是 US。从下拉列表中选择国家/地区代码。
- **州或省** (ST) - 证书中包括的州或省。
- **地区或城市** (L) - 证书中包括的地区，例如城市名称。
- **组织** (O) - 证书中包括的组织或公司名称。
- **组织单位（部门）** (OU) - 证书中包含的组织单位名称（例如部门名称）。
- **通用名称** (CN) - 证书中包括的 X.500 通用名称。它们可能是设备、网站或其他文本字符串的名称。通常需要有此元素，才能成功进行连接。例如，用于远程访问 VPN 的内部证书中必须包括 CN。
- **密钥类型** - 要为此证书生成的密钥的类型：RSA、ECDSA（椭圆曲线数字签名算法）或 EDDSA（爱德华兹曲线数字签名算法）。
- **密钥大小** - 要生成的密钥的大小。通常，较长的密钥更安全。但是，生成模数较大的密钥需要更长的时间，而且交换时的处理时间也更长。允许的大小因密钥类型而异。
  - RSA 密钥可以是 2048、3072 或 4096 位。
  - ECDSA 密钥可以是 256、384 或 521 位。

    EDDSA 密钥可以是 256 位。
- **有效期** - 证书将被视为有效的时间段。无论您如何设置到期日期，默认设置为 825 天（从今天起）。点击**设置默认值**可恢复为默认值。您可以通过以下任一方法配置该时间段。请务必在证书过期前进行更换。
  - **按日期** - 点击**到期日期**，然后选择证书应被视为有效的最后一天。
  - **按天数** - 输入从今天起证书应被视为有效的天数。输入数字后，您可以点击**按日期**查看计算得出的到期日期。

步骤 5 单击**保存**。

上传受信任的 CA 证书

受信任证书颁发机构 (CA) 证书用于签署其他证书。它是自签名证书，也称为根证书。由另一个 CA 证书颁发的证书称为从属证书。

有关使用这些证书的功能的信息，请参阅功能使用的证书类型，第 2 页。

受信任 CA 证书可从外部证书颁发机构获取，也可以使用自己的内部 CA 创建（例如通过 OpenSSL 工具生成证书）。然后，使用以下步骤程序上传证书。

开始之前

系统会每天联系思科一次，以确定是否有新的或更新的受信任 CA 证书，并在可用时下载更新后的证书。这一日常检查可确保预安装的证书都保持最新。您可以使用 **show cert-update** 命令在 CLI 中监控此自动检查。您可以使用 **configure cert-update auto-update disable** 命令来禁用日常检查，并可以使用 **configure cert-update run-now** 命令来手动下载更新。

过程

步骤 1 选择**对象**，然后从目录中选择**证书**。

步骤 2 执行以下操作之一：

- 依次点击 + > **添加受信任 CA 证书**。
- 要编辑证书，请点击证书的编辑图标 ()。

步骤 3 键入证书的**名称**。

该名称仅在配置中用作对象名称，不会成为证书本身的一部分。

步骤 4 点击**上传证书**（或在编辑时点击**替换证书**），然后选择受信任CA证书文件（例如*.pem）。允许的文件扩展名有 .pem、.cert、.cer、.crt 和 .der。或者，粘贴到受信任 CA 证书中。

证书中的服务器名称必须与服务器主机名/IP 地址匹配。例如，如果使用 10.10.10.250 作为 IP 地址，但证书中的地址为 ad.example.com，则连接失败。

该证书必须为 PEM 或 DER 格式的 X509 证书。

您粘贴的证书必须包括 BEGIN CERTIFICATE 和 END CERTIFICATE 行。例如：

```
-----BEGIN CERTIFICATE-----
MIIFgTCCA2mgAwIBAgIJANvdcLnabFGYMA0GCSqGSIb3DQEBCwUAMFcxCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJUWDEPMA0GA1UEBwwGYXVzdGluMRQwEgYDVQQKDAsx
OTIuMTY4LjEuMTEUMBIGA1UEAwwLMTkyLjE2OC4xLjEwHhcNMTYxMDI3MjIzNDE3
WhcNMTcxMDI3MjIzNDE3WjBXMQswCQYDVQQGEwJVUzELMAkGA1UECAwCVFgxDzAN
BgNVBAcMBmF1c3RpbjEUMBIGA1UECgwLMTkyLjE2OC4xLjExFDASBgNVBAMMCzE5
Mi4xNjguMS4xMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA5NceYwtP
```

```
ES6Ve+S9z7WLKGX5JlF58AvH82GPkOQdrixn3FZeWLQapTpJZt/vgtAI2FZIK31h
(...20 lines removed...)
hbr6HOgKlOwXbRvOdksTzTEzVUqbgxt5Lwupg3b2ebQhWJz4BZvMsZX9etveEXDh
PY184V3yeSeYjbSCF5rP71fObG9Iu6+u4EfHp/NQv9s9dN5PMffXKieqpuN20Ojv
2b1sfOydf4GMUKLBUMkhQnip6+3W
-----END CERTIFICATE-----
```

步骤 5 如果此证书不是由证书颁发机构颁发，请选择**跳过 CA 证书检查 (Skip CA Certificate Check)**。

如果需要将本地 CA 证书安装为受信任的 CA 证书，请跳过此复选框。

步骤 6 设置**验证使用**以限制证书的使用。

某些功能允许您选择是否可以根据特定证书验证连接。您必须在证书中指出这些功能可以有效使用证书，否则连接将被拒绝。

这些选项中未包含的任何功能都可以根据此证书进行验证，而无需明确的使用许可。例如，SSL 解密策略和托管 设备管理器的 Web 服务器会忽略“验证使用”选项。如果您在此字段中选择任何选项，证书将下载到使用 **show running-config** 命令显示的运行配置。

这些选项的主要目的是阻止您建立 VPN 连接，因为它们可以根据特定证书进行验证。

- **SSL 服务器** - 验证远程 SSL 服务器上的证书。用于动态 DNS。
- **SSL 客户端** - 验证远程访问 VPN 传入连接的证书。
- **IPsec 客户端** - 验证 IPsec 站点间 VPN 传入连接的证书。
- **其他** - 验证 LDAPS 等不受 Snort 检测引擎管理的功能。仅当特定功能存在问题时，才选择此选项。**其他**与所有其他选项只能二选其一：您必须先取消选择**其他**，然后才能选择任何其他选项，而且必须先取消选择所有选项，然后才能选择**其他**。

步骤 7 点击**确定 (OK)**。

配置受信任 CA 证书组

使用 SSL 解密策略设置中的外部受信任 CA 证书组指定 SSL 解密策略应信任哪些证书。如果最终用户尝试连接到证书颁发机构的证书不在受信任证书中的站点，则用户会收到一条消息，要求信任该证书。因此，不将证书放在受信任列表中会给最终用户带来不便，但这本身并不能阻止连接（您可以使用访问控制规则来完成连接）。

默认组为 Cisco-Trusted-Authorities。仅在以下情况下，您才需要创建自己的组：

- 您希望信任不在默认组中的证书。然后，您可以在 SSL 解密策略设置中选择默认组和新组。
- 您希望信任的证书列表比默认组限制更严格。然后，您将创建一个具有受信任证书的完整列表（而不只是您所增加的受信任证书）的组，并将其选择为 SSL 解密策略设置中的唯一组。

开始之前

上传您将添加到组中的所有受信任 CA 证书（如果它们尚未进入系统中）。

过程

步骤 1 选择**对象**，然后从目录中选择**证书**。

步骤 2 执行以下操作之一：

- 要创建新证书组，请点击 并选择**添加证书组**。
- 要编辑证书组，请点击该组的编辑图标 ( )。

步骤 3 为证书组输入**名称**和说明（后者为可选项）。

步骤 4 点击 + 将证书添加到组。

在组中添加您需要的所有证书。在构建组时，您可以点击**创建新的受信任 CA 证书**以上传新证书。

如果您不再需要组中的证书，请点击证书的 X 图标（右侧）。

步骤 5 点击**确定 (OK)**。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。