CTI OS Security

This chapter provides information about configuring the CTI OS Security Certificate and the Security Compatibility.

CTI OS Security Certificate Configuration

The CTI OS Security Certificate comprises the following:

- CTI OS Security Setup programs.
- Signing CTI Toolkit Desktop Client Certificate Request with Self-Signed Certificate Authority (CA).
- Signing CTI OS Server Certificate Request with Self-Signed CA.
- Signing CTI Toolkit Desktop Client Certificate Request with Third-Party CA.
- Signing CTI OS Server Certificate Request with Third-Party CA.

Each of these entities is detailed in this section.

Note Both Certificate Revocation List (CRL) and certificate chain are not supported in CTI OS Security.

CTI OS Security Setup Programs

To configure the CTI OS, three setup programs are implemented. These setup programs are part of the Win32 CTI OS toolkit installation, and are located in the directory `<drive>:\Program Files\Cisco Systems\CTIOS Client\CTIOS Security\Utilities`.

The first setup program, CreateSelfSignedCASetupPackage.exe, creates a self-signed certificate authority (CA). This must be run once if the customer wants to use a self-signed CA instead of a third party and the output of CreateSelfSignedCASetupPackage.exe must be saved in a secure place. This program creates CA-related files. One file, CtiosRoot.pem, contains the private CA information. This file must be kept in a safe place. Another file, CtiosRootCert.pem, contains public CA information. This setup program asks the

user to enter a password for the CA (between 8 and 30 characters), which are used when signing CTI OS certificate requests.

The second setup program, SecuritySetupPackage.exe, is used to generate certificate requests for both CTI Toolkit Desktop Client and CTI OS Server. If the certificate request is for the CTI OS Server, then it generates CtiosServerKey.pem, and CtiosServerReq.pem. These files are used when signing server certificates. If the certificate request is for the CTI Toolkit Desktop Client, then it generates CtiosClientkey.pem, and CtiosClientreq.pem. These files are used when signing client certificates.

The third setup program, SignCertificateSetupPackage.exe. is used to sign both CTI Toolkit Desktop Client and CTI OS Server certificates. This program is used only when the customer decides to sign their CTI Toolkit Desktop Client and CTI OS Server certificates with self signed CA. This program must reside in the same directory as the CtiosRootCert.pem and CtiosRoot.pem. If the certificate that is going to be signed is for the client, it generates CtiosClient.pem file. If the certificate that is going to be signed is for the server, it generates CtiosServer.pem file. This program asks the user to enter the following information:

- Ctios Certificate Authority Password. This password is the one used to create a self-signed CA.
- Select either CTI Toolkit Desktop Client Certificate Request or CTI OS Server Certificate Request.

Sign CTI Toolkit Desktop Client Certificate Request with Self-Signed CA

Note Generate CtiosRootCert.pem only once; use the same file for CTI OS server and client machines.

Follow these steps to sign a CTI Toolkit Desktop Client certificate request.

Procedure

Step 1 If the self-signed CA does not exist, then run CreateSelfSignedCASetupPackage.exe and store all the files that were created by the CreateSelfSignedCASetupPackage.exe program in a safe place. This step generates CtiosRoot.pem and CtiosRootCert.pem in the same folder from where the setup is run.

Step 2 Copy CtiosClientkey.pem and CtiosClientreq.pem files from the CTI Toolkit Desktop Client machine to the machine where CtiosRoot.pem and CtiosRootCert.pem reside.

Note You must Copy the Ctiosclientkey.pem and CtiosClientreq.pem files from the CTI Toolkit Desktop Client machine under `<drive>:\Program Files\Cisco Systems\CTIOS Client\CTIOS Security` to the folder where CtiosRoot.pem and CtiosRootCert.pem resides.

Step 3 Run SignCertificateSetupPackage.exe from the same directory where CtiosClientkey.pem, CtiosClientreq.pem, CtiosRoot.pem, and CtiosRootCert.pem reside, select CTIOS Client Certificate Request, and enter the "Ctios Certificate Authority password."
This step generates the file CtiosClient.pem if it is successful; otherwise it displays an error message.

Step 4 Copy both CtiosClient.pem and CtiosRootCert.pem back to the machine where CTI Toolkit Desktop Client is installed and save them in the `<drive>:\Program Files\Cisco Systems\CTIOS Client\CTIOS Security` directory.

Step 5 Delete CtiosClientkey.pem in `<drive>:\Program Files\Cisco Systems\CTIOS Client\CTIOS Security\Utilities` directory from the machine where CTI Toolkit Desktop Client is installed.

Step 6 Delete CtiosClientkey.pem, CtiosClientreq.pem, and CtiosClient.pem from the machine where SignCertificateSetupPackage.exe ran.

Sign CTI OS Server Certificate Request with Self-Signed CA

Note Generate CtiosRootCert.pem only once; use the same file for CTI OS server and client machines.

Follow these steps to sign a CTI OS Server certificate request.

Procedure

Step 1 If the self-signed CA does not exist, then run CreateSelfSignedCASetupPackage.exe and store all the files that were created by the CreateSelfSignedCASetupPackage.exe program in a safe place. This step generates CtiosRoot.pem and CtiosRootCert.pem in the same folder from where the setup is run.

Step 2 Copy CtiosServerKey.pem and CtiosServerReq.pem files from the CTI OS Server machine to the machine where CtiosRoot.pem and CtiosRootCert.pem reside.

Note You must copy both CtiosServerKey.pem and CtiosServerReq.pem files from the CTI OS server machine under *<drive>*:\icm\Instance name\CTIOS1\Security to the same directory as CtiosRoot.pem and CtiosRootCert.pem.

Step 3 Run SignCertificateSetupPackage.exe from the same directory where CtiosServerKey.pem, CtiosServerReq.pem, CtiosRoot.pem, and CtiosRootCert.pem reside, select CTIOS Server Certificate Request, and enter the "Ctios Certificate Authority password."
This step generates CtiosServer.pem file if it is successful; otherwise it displays an error message.

Step 4 Copy both CtiosServer.pem and CtiosRootCert.pem back to the machine where CTI OS Server resides and save them in the *<drive>*:\icm*Instance name*\CTIOS1\Security directory.

Step 5 Delete CtiosServerkey.pem under *<drive>*:\icm\Instance name\CTIOS1\Security from the machine where CTI OS Server is installed.

Step 6 Delete CtiosServerKey.pem, CtiosServerReq.pem, and CtiosServer.pem from the machine where SignCertificateSetupPackage.exe ran.

Step 7 If CTIOS Server has peer server, then:

a) Copy CtiosClientkey.pem and CtiosClientreq.pem files from the CTI OS Server machine to the machine where CtiosRoot.pem and CtiosRootCert.pem reside. You must copy both CtiosClientkey.pem and CtiosClientreq.pem files to the same directory as CtiosRoot.pem and CtiosRootCert.pem.

b) Run SignCertificateSetupPackage.exe from the same directory where CtiosClientkey.pem, CtiosClientreq.pem, CtiosRoot.pem, and CtiosRootCert.pem reside, select **CTI Toolkit Desktop Client Certificate Request**, and enter the "Ctios Certificate Authority password." This step generates CtiosClient.pem file if it is successful; otherwise it displays an error message.

c) Copy CtiosClient.pem to the machine where CTI OS Server resides and save it in *<drive>*:\icm\<*Instance name*>\CTIOS1\Security directory.

d) Delete CtiosClientkey.pem from the machine where CTI OS Server is installed.

e) Delete CtiosClientkey.pem, CtiosClientreq.pem, and CtiosClient.pem from the machine where SignCertificateSetupPackage.exe ran.

Sign CTI Toolkit Desktop Client Certificate Request with Third-Party CA

Procedure

Step 1 Copy CtiosClientreq.pem file from the CTI Toolkit Desktop Client machine to the machine where the third-party CA resides.

Step 2 Signing CTI Toolkit Desktop Client certificate request (CtiosClientreq.pem) with third-party CA generates a CTI Toolkit Desktop Client certificate. Rename it CtiosClientCert.pem.

Step 3 The third-party CA has its certificate public information in a file. Rename this file CtiosRootCert.pem.

Step 4 Copy both CtiosClientCert.pem and CtiosRootCert.pem to the machine where CTI Toolkit Desktop Client resides and save them in the `<drive>:\Program Files\Cisco Systems\CTIOS Client\Security` directory.

Step 5 On the CTI Toolkit Desktop Client machine, copy the data in CtiosClientCert.pem and the data in CtiosClientkey.pem files into one file called CtiosClient.pem. The order is very important, so CtiosClient.pem must contain CtiosClientCert.pem data first and then CtiosClientkey.pem data second.

Step 6 Delete CtiosClientCert.pem and CtiosClientkey.pem from the CTI Toolkit Desktop Client machine.

Sign CTI OS Server Certificate Request with Third-Party CA

Follow these steps to sign a CTI OS Server certificate request.

Procedure

Step 1 Copy CtiosServerReq.pem file from the CTI OS Server machine to the machine where the third-party CA resides.

Step 2 Signing CTI OS Server certificate request (CtiosServerReq.pem) with third-party CA generates a CTI OS Server certificate. Rename it CtiosServerCert.pem.

Step 3 The third-party CA has its certificate public information in a file. Rename this file CtiosRootCert.pem.

Step 4 Copy both CtiosServerCert.pem and CtiosRootCert.pem to the machine where CTI OS Server resides and save them in the `<drive>:\icm\<Instance name>\CTIOS1\Security` directory.

Step 5 On the CTI OS Server machine, copy the data in CtiosServerCert.pem and the data in CtiosServerkey.pem files into one file called CtiosServer.pem. The order is very important, so CtiosServer.pem must contain CtiosServerCert.pem data first and then CtiosServerkey.pem data second.

Step 6 Delete CtiosServerCert.pem and CtiosServerkey.pem from the CTI OS Server machine.

Step 7 If CTIOS Server has peer server, then:

a) Copy CtiosClientreq.pem file from the CTI OS Server machine to the machine where the third party CA resides.

b) Signing CTI Toolkit Desktop Client certificate request (CtiosClientreq.pem) with third party CA generates a CTI Toolkit Desktop Client certificate. Rename it CtiosClientCert.pem.
c) Copy CtiosClientCert.pem file to the machine where CTI OS Server resides and save it in the `<drive>:\icm\<Instance name>\CTIOS1\Security` directory.
d) On the CTI OS Server machine, copy the data in CtiosClientCert.pem, and the data in CtiosClientkey.pem files into one file called CtiosClient.pem. *You must copy the files in this order*, so that CtiosClient.pem contain CtiosClientCert.pem data first and then CtiosClientkey.pem data second.
e) Delete CtiosClientCert.pem and CtiosClientkey.pem from the CTI OS Server machine.

CTI OS Security Passwords

CTI OS Security introduces five types of passwords:

1. CTI OS Client certificate password: The administrator or installer enters this password when installing CTI OS Client security. This password is used for the CTI OS Client certificate request private key and it can be anything and the administrator or installer need not remember it.
2. CTI OS Server certificate password: The administrator or installer enters this password when installing CTI OS Server security. This password is used for the CTI OS Server certificate request private key and it can be anything and the administrator or installer need not remember it.
3. CTI OS Peer certificate password: The administrator or installer enters this password when installing CTI OS Server security. This password is used for the CTI OS Peer Server certificate request private key and it can be anything and the administrator or installer need not remember it.
4. Monitor Mode password: The administrator or installer enters this password when installing CTI OS Server security. This password is used by the agents when connecting to a secure CTI OS Server using CTI OS monitor mode applications such as AllAgents and AllCalls. This password must be the same on both CTI OS Peer Servers and the administrator or installer and whoever is using the CTI OS monitor mode applications must remember it.
5. Certificate Authority (CA) password: The administrator or installer enters this password when creating self-signed CA. The password can be anything and the administrator or installer must remember it because they must use it every time that this CA signs a certificate request.

CTI OS Security Registry Keys

The registry keys located at `[HKEY_LOCAL_MACHINE\SOFTWARE\CiscoSystems, Inc.\CTIOS\<CTIOS_Instancename>\CTIOS1\Server\Security]` define the settings for CTI OS Server Security.

Table 1: Registry Values for CTI OS Server

Registry Value Name	Value Type	Description	Default
AuthenticationEnabled	DWORD Value	For more information, see Authentication Mechanism, on page 8.	1

Registry Value Name	Value Type	Description	Default
CAType	DWORD Value	Is created at install time. A value of 1 means the chosen CA type is self signed, and a value of 2 means the chosen CA type is third party.	1
NumBytesRenegotiation	DWORD Value	Is used for session renegotiation, which means requesting a handshake to be performed during an already established connection. This causes CTI OS Client credentials to be reevaluated and a new session to be created. It is important to replace the session key periodically for long-lasting SSL connections, because doing so makes the connection between the CTI OS Server and CTI OS Client more secure. Renegotiation happens after the CTI OS Server sends 10000000 bytes to the CTI OS Client. The minimum and the default value are 10000000.	10000000
SecurityEnabled	DWORD Value	Is created at install time. A value of 1 means CTI OS Security is enabled, and a value of 0 means CTI OS Security is disabled.	0
MonitorModeDisableThreshold	DWORD Value	Controls the number of consecutive failed attempts to access monitor mode functionality before monitor mode is disabled. **Note** For more information, see "Monitor Mode Security."	3 (default)
MonitorModeDisableDuration	DWORD Value	Controls the length of time to disable monitor mode functionality after the configured number of consecutive failed attempts to access monitor mode functionality have occurred. **Note** For more information, see "Monitor Mode Security."	15 minutes (default)

The registry keys located at [`HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTI OS Client`] define the settings for CTI OS Client Security. The following table lists the registry values for these keys.

Table 2: Registry Values for CTI OS Client

Registry Value Name	Value Type	Description	Default
CAType	DWORD Value	Is created at install time. A value of 1 means the chosen CA type is self signed, and a value of 2 means the chosen CA type is third party.	1
HandShakeTime	DWORD Value	Is created at install time. This key defines how long the CTI OS client waits during the SSL/TLS handshake phase.	5

Mode Security Monitoring

When the CTI OS Server has security enabled, the server guards itself against unlawful attempts to gain access to monitor mode functionality. It does this by tracking the number of failed attempts to access monitor mode functionality. After the configured number of consecutive failed attempts to access monitor mode functionality have occurred (3 by default), the CTI OS Server disables monitor mode functionality. When this happens, all attempts to access monitor mode functionality fail. This occurs until the configured period of time after the last failed attempt to access monitor mode functionality has passed. This time period is 15 minutes by default.

The *MonitorModeDisableThreshold* and the *MonitorModeDisableDuration* registry settings have been added to the `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\Ctios\CTIOS<instance>\<ServerName>\Server\Security` to allow you to modify the defaults.

MonitorModeDisableThreshold
: This registry field is a DWORD. It controls the number of consecutive failed attempts to access monitor mode functionality before monitor mode is disabled.

MonitorModeDisableDuration
: This registry field is a DWORD. It controls the length of time to disable monitor mode functionality after the configured number of consecutive failed attempts to access monitor mode functionality have occurred.

Security Compatibility

Passing data over the network in a secure way is vital to both Cisco and the customer. CTI OS implements these features to deal with security:

Wire Level Encryption
: To help secure all the traffic between the CTI OS Server and the CTI OS Client using Transport Layer Security (TLS). This protocol provides encryption and certification at the transport layer (TCP).

Authentication mechanism
: For Unified CCE only, makes sure that an agent logs in successfully only if the agent supplies the correct password.

Wire Level Encryption

Wire Level Encryption provides an encryption mechanism between the latest version of CTI OS Server and CTI OS Client 11.x (y). By default, Wire Level Encryption is turned OFF. If the value of "SecurityEnabled" registry key is 0, then security is off. If the value of "SecurityEnabled" registry key is 1, then security is on. This key exists under:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems,
Inc.\Ctios\CTIOS_<InstanceName>\CTIOS1\Server\Security
```

If the security is turned on in the CTI OS Server, then the CTI OS clients using .NET CIL, or Java CIL cannot connect to the CTI OS Server. If security is on in one CTI OS Server and this server has peers, then you must turn on security in the peers as well. The following table contains the list of CTI OS toolkits.

Table 3: Wire Level Encryption: List of CTI OS Toolkits

	C++ CIL Toolkit	COM CIL Toolkit	Java CIL Toolkit	.NET CIL Toolkit
Support Wire Level Encryption	Yes	Yes	No	No

Authentication Mechanism

The authentication mechanism is for Unified CCE only. It is on by default. If the value of "AuthenticationEnabled" registry key is 0, then authentication is off. If the value of "AuthenticationEnabled" registry key is 1, then authentication is on. This key exists under:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems,
Inc.\Ctios\CTIOS_<InstanceName>\CTIOS1\Server\Security
```

For all peripherals other than Unified CCE, this registry key is not used.