Get Started with the Log Forwarding App

If you need to fulfill your organization's legal compliance requirements, the Log Forwarding app enables you to easily forward logs stored in Cortex Data Lake to external destinations. For example, you can forward logs using Syslog to a SIEM for long term storage, SOC, or internal audit obligations, and forward email notifications for critical events to an email address. Logs generated by the firewall, Traps, Cortex XDR - Analytics, and Cortex XDR - Investigation and Response can all be forwarded to a Syslog or email destination.

- Add Log Forwarding App Instance
- Forward Logs from Cortex Data Lake to a Syslog Server
- Forward Logs from Cortex Data Lake to an Email Server
- Log Record Formats
- Specify What Log Types to Forward
- List of Trusted Certificates for the Log Forwarding App
Add a Log Forwarding App Instance

Log Forwarding is included with Cortex Data Lake and does not require any additional licensing. Before you can use Log Forwarding, you must activate it on the Cortex hub. After you activate the app, you can add a Log Forwarding app instance to the Cortex hub. Although you only need to activate the Log Forwarding app one time, you must add a separate Log Forwarding app instance for each instance of Cortex Data Lake you’ve purchased. Each instance of the Log Forwarding app can forward logs to a single destination, and you can associate it with only one instance of Cortex Data Lake.

In addition, before you can activate or add a Log Forwarding app instance, you must have the right administrator role. If you do not have the correct role, you will not be able to see or manage either Cortex Data Lake or the Log Forwarding app from the Cortex hub.

Use the following workflow to activate the Log Forwarding App and add an instance of the app.

**STEP 1 | Sign In** to the Cortex hub at https://apps.paloaltonetworks.com/.

If you do not see Cortex Data Lake or the Log Forwarding app as available Palo Alto Networks apps, have the Superuser on your support account use the Cortex hub to **assign you the role you need** to activate and access the app.

**STEP 2 | To activate the Log Forwarding app**, select the Log Forwarding app tile and click **Activate**.

This is a one-time task for your customer account. If you have already activated the app, go to the next step.

**STEP 3 | Select the gear icon** and then **Add Instance** to add a new Log Forwarding app instance.
Your company name and the license type displays on the Activate Log Forwarding page.

**STEP 4** | Enter an **Instance Name** (up to 63 characters) and a **Description** to help you identify the Log Forwarding app instance.

**STEP 5** | Select the **Region** in which you have deployed the Cortex Data Lake instance from which you want to forward logs.

*The Logging Service is now called Cortex Data Lake. In some locations, such as this one, you might still see the Logging Service name.*

**STEP 6** | Choose an available **Logging Service** instance from the region you selected.

A Cortex Data Lake (Logging Service) instance can forward logs to only one Log Forwarding app. The drop-down displays Cortex Data Lake instances that are running (●) and shows you which instances are available and which are attached to an instance of the Log Forwarding app.

**STEP 7** | Click **Agree and Activate**, to accept the terms of the End User License Agreement.

The app instance is launched, and the status indicates when the app is available for configuration.

**STEP 8** | Continue to **Forward Logs from Cortex Data Lake to a Syslog Server** and **Forward Logs from Cortex Data Lake to an Email Server**.
Forward Logs from Cortex Data Lake to a Syslog Server

To meet your long term storage, reporting and monitoring, or legal and compliance needs, you can configure the Log Forwarding app to forward all logs or a subset of logs to a Syslog receiver. The Log Forwarding app uses the IETF Syslog message format defined in RFC 5425 to forward logs. For each instance of Cortex Data Lake, you can deploy one instance of the Log Forwarding app and forward logs to ten Syslog destinations.

The communication between the Log Forwarding app and the Syslog destination uses Syslog over TLS, and upon connection the Log Forwarding app validates that the Syslog receiver has a certificate signed by a trusted root CA. To complete the SSL handshake and establish the connection, the Syslog receiver must present all the certificates in the chain of trust.

The Log Forwarding app does not support self-signed certificates.

**STEP 1 | Enable communication between the Log Forwarding app and your Syslog receiver.**

Ensure that your Syslog receiver can connect to the Log Forwarding app and can present a valid CA certificate to complete the connection request.

- Allow an inbound TLS feed to your Syslog receiver from the following IP address ranges:

<table>
<thead>
<tr>
<th>Country</th>
<th>IP Address Ranges</th>
</tr>
</thead>
<tbody>
<tr>
<td>US</td>
<td>65.154.226.0/24</td>
</tr>
<tr>
<td></td>
<td>34.67.106.64/28</td>
</tr>
<tr>
<td>EU</td>
<td>154.59.126.0/24</td>
</tr>
<tr>
<td></td>
<td>34.90.138.80/28</td>
</tr>
</tbody>
</table>

*If you have whitelisted specific IP addresses for inbound traffic, you must also whitelist the above IP address ranges to forward logs to your Syslog receiver.*

- Obtain a certificate from a well known, public CA and install it on your Syslog receiver.

  Because the Log Forwarding app validates the server certificate to establish a connection, you must verify that the Syslog receiver is configured to properly send the SSL certificate chain to the Log Forwarding app. If the app cannot verify that the certificate of the receiver and all CA’s in the chain are trustworthy, the connection cannot be established. See List of Trusted Certificates for the Log Forwarding App.

**STEP 2 | Sign In to the Cortex hub at https://apps.paloaltonetworks.com/**
STEP 3 | Select the Log Forwarding app instance that you want to configure for Syslog forwarding.

If you have multiple Log Forwarding app instances, hover over the Log Forwarding tile and select an instance from the list of those available.

STEP 4 | Select Syslog > Add to add a new Syslog Forwarding profile.

![Syslog Forwarding](image)

STEP 5 | Enter a descriptive Name for the profile.

STEP 6 | Enter the Syslog Server IPv4 address or FQDN.

STEP 7 | Enter the Port on which the Syslog server is listening.

The default port for Syslog messages over TLS is 6514.

STEP 8 | Select the Facility.

Choose one of the Syslog standard values. The value maps to how your Syslog server uses the facility field to manage messages. For details on the facility field, see RFC 5424 (IETF format).

STEP 9 | To receive a Status Notification when the Log Forwarding app is unable to connect to the Syslog server, enter the email address at which you’d like to receive the notification.

These notifications describe the error impacting communication between the Log Forwarding app and the Syslog server, so that you can take the appropriate steps to restore Syslog connectivity.

*Step 12 in this workflow gives you the option to enable the Log Forwarding app to default to email forwarding if it is unable to connect to any Syslog servers.*

STEP 10 | Select the logs you want to forward.

You can specify the log vendor (the source that is sending logs to Cortex Data Lake), log types and either define a custom filter or use the predefined filters to forward the log types that are most important to you (here’s more details on predefined and custom filters, including examples of custom filters you might want to build).
1. **Add** to select the **Log Vendor**.
   The log vendors are the sources that generated the logs, such as Firewall or Traps.

2. **Select the Log Type**.

   *The Threat log type does not include WildFire logs, URL logs, or Data logs. If you wish to forward these log types, you must add them individually.*

   You can only select one log subtype at a time.

   *After you select the Log Type you want to forward, the predefined filter shows as selected by default. If you want to forward all logs associated with the log type you’ve selected, leave Predefined selected and continue to save this rule without adding any filters. Otherwise, continue to the next step to specify if you want to forward a subset of logs.*

3. **(Optional)** Use the **Filter** to forward only the logs that are most critical to you.

   For each log type, you can set the **Filter** to your custom needs or use the predefined options.

   ![Forwarding](image)

   With the **Predefined** filter, you can opt to **Send Prisma Access firewall logs only**. Use this option if you are using Prisma Access to secure your remote networks or mobile users, and want to forward logs generated by the firewalls that belong to this service only.

   For details on the filtering options, review how to **Custom Log Filters**.

4. **Save** your changes.

5. Add other log types that you’d like to forward.

**STEP 11** | **Save** your changes.

**STEP 12** | Decide if you want to **Continue forwarding logs via email if syslog forwarding is unavailable**.

The Log Forwarding app prioritizes Syslog forwarding. Therefore, even when you have configured email forwarding profile(s), when it is unable to establish a connection to a Syslog server that you have defined, it completely stops forwarding logs and queues the logs. When you select this option, the Log Forwarding app continues with email forwarding when it is unable to connect to any Syslog servers defined in your profiles instead of queueing them up so that you receive notifications at an external destination. And when Syslog connectivity is restored, the app resumes forwarding new logs stored to the Syslog server.
To ensure that you do not lose logs, make sure to set up email log forwarding before you enable this option. See Forward Logs from Cortex Data Lake to an Email Server.

**STEP 13** | Verify that the Log Forwarding app instance reports Status as Running (○).

*If you need to stop forwarding logs, select Settings (○) on the Cortex hub, hover over the app instance and click Stop. This allows you to temporarily suspend log forwarding, but your configuration is retained and you can Resume log forwarding again. When you resume forwarding, you may experience a delay before the Syslog receiver starts receiving logs again.*

**STEP 14** | Verify that you can view logs on the Syslog receiver.

For detailed information about the log format, refer to the Syslog field descriptions:

- **PAN-OS 8.1**

  *Regardless of whether the firewalls are running PAN-OS 8.0 or 8.1, the log format on the Syslog receiver matches the PAN-OS 8.1 format.*

- **Traps management service**
Forward Logs from Cortex Data Lake to an Email Server

To get email notifications whenever critical issues occur on your network, you can configure the Log Forwarding app to send notifications to an email destination. The Log Forwarding app uses the Palo Alto Networks SMTP server to forward log information in an email format, and all emails are sent from noreply@cs.paloaltonetworks.com. The communication between the Log Forwarding app and the email destination uses SMTP over TLS, and SMTP server certificate is signed by a trusted root CA.

For each instance of Cortex Data Lake, you can one deploy an instance of the Log Forwarding app and set up log forwarding to email and Syslog destinations.

**STEP 1** | **Sign In** to the Cortex hub at [https://apps.paloaltonetworks.com/](https://apps.paloaltonetworks.com/).

**STEP 2** | Select the Log Forwarding app instance that you want to configure for email forwarding.

If you have multiple Log Forwarding app instances, hover over the Log Forwarding tile and then select an instance from the list of available instances.

**STEP 3** | Configure email forwarding.

You cannot add your SMTP server to the Log Forwarding app currently.

1. Select **Email > Add** to add a new email forwarding profile.
2. Enter a descriptive **Name** for the profile.
3. Enter the email address of the administrator **To whom you want to send email**.
   
   You can include another email address to include as **BCC**.
4. Enter the **Email Subject** to clearly identify the purpose of the notification.
5. Select the logs you want to forward.

   You can specify the log vendor (the source that is sending logs to Cortex Data Lake), log types and either define a custom filter or use the predefined filters to forward the log types that are most important to you (here's more details on predefined and custom filters, including examples of custom filters you might want to build).

   1. **Add** to select the **Log Vendor**.

      The log vendors are the sources that generated the logs, such as Firewall or Traps.

   2. **Select the Log Type**.

      You can only select one log subtype at a time.

      *After you select the Log Type you want to forward, the predefined filter shows as selected by default. If you want to forward all logs associated with the log type you’ve selected, leave Predefined selected and continue to save this rule without*
adding any filters. Otherwise, continue to the next step to specify if you want to forward a subset of logs.

3. (Optional) Use the Filter to forward messages for only the logs that are most critical to you.

For each log type, you can customize the Filter for your needs or use the predefined options.

With the Predefined filter, you can opt to Send Prisma Access firewall logs only. Use this option if you are using Prisma Access to secure your remote networks or mobile users, and want to forward logs generated by the firewalls that belong to this service only.

For details on the filtering options, review how to Custom Log Filters.

4. Save your changes.

5. Add other log types for which you'd like to receive email notifications.

6. Save your changes.

Check your email to verify that you have received a test email from noreply@cs.paloaltonetworks.com.

Email forwarding is rate limited to allow 10 emails per second.

STEP 4 | Decide if you want to receive email notifications when the connection to the Syslog destination is down.

If you have configured Syslog forwarding, the Log Forwarding app completely stops forwarding logs and emails when it is unable to connect to any of the Syslog server that you have defined. The app queues the logs and resumes email and Syslog forwarding when the Syslog connection is reestablished. If you would like to continue receiving email notification when the Log Forwarding app is disconnected from the Syslog servers defined in your profiles, select Syslog > Continue forwarding logs via email if syslog forwarding is unavailable. If you enable this option, you will receive email notifications for the events you have configured above when the Syslog connectivity is down, but when the connection between the
Syslog server and the Log Forwarding app is restored, the logs generated during the time interval that the connection was down are not forwarded to the Syslog destinations.

**STEP 5 | Verify that the Log Forwarding app instance reports Status as Running (✓).**

*If you need to stop forwarding logs, select Settings (⚙️) on the Cortex hub, hover over the app instance and click Stop. This allows you to temporarily suspend log forwarding, but your configuration is retained and you can Resume log forwarding again. When you resume forwarding, you may experience a delay before the Syslog receiver starts receiving logs again.*
Log Record Formats

The format of the log records you forward depends on the vendor that generates the logs. Here’s where you can find information on the Syslog and email outputs you can expect receive, as well as descriptions of log fields.

<table>
<thead>
<tr>
<th>Log Vendor/Source</th>
<th>Where to find more information about the logs:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>• PAN-OS 9.0 Syslog Field Descriptions</td>
</tr>
<tr>
<td>Traps</td>
<td>• Traps log field descriptions</td>
</tr>
<tr>
<td>Cortex XDR - Analytics</td>
<td>• Cortex XDR - Analytics Log Fields and Formats</td>
</tr>
<tr>
<td>Cortex XDR - Investigation and Response</td>
<td>• Cortex XDR - Investigation and Response Log Fields and Formats</td>
</tr>
</tbody>
</table>
Specify What Log Types to Forward

You can specify the logs you want to forward based on log type and the data contained in log fields. You'll need to do this when you're first setting up log forwarding to a syslog or an email server. However, you can add to or adjust the log types you’re forwarding at any time.

- Add or Adjust a Log Filter
- Predefined Log Filters
- Custom Log Filters
- Log Forwarding Filters for Firewall Logs
- Log Forwarding Filters for Traps Logs
- Log Forwarding Filters for Cortex XDR Alerts

Add or Adjust a Log Filter

You can use log forwarding filters to forward only the logs that are most important to you. You have the option to define log filters when you're first setting up log forwarding to an email or syslog destination. But you can also add or adjust your log filters at any time.

STEP 1 | Log in to the Log Forwarding app, and choose a syslog or email forwarding profile to modify.

STEP 2 | Add or modify a Forwarding filter:
STEP 3 | Choose the vendor from which you want to forward logs—the firewall, Traps, Cortex XDR - Analytics, or Cortex XDR - Investigation & Response—and also the log type to forward.

STEP 4 | Now you can decide if you want to forward all logs, or if you want to filter the logs that are most important to you.

- **To forward certain logs:**
  To forward logs based on log fields like alert severity or threat type, you can use [Predefined Log Filters](#) that are built-in to the Log Forwarding app, or you can create [Custom Log Filters](#).

- **To forward all logs:**
  After selecting the Log Type, **Save** the forwarding rule. You'll see that Predefined is selected by default; that's okay—continue to save the rule. After saving, you'll see that the filter is set to forward "All Logs" of the log type you selected.
Predefined Log Filters

The Log Forwarding app can help you to easily specify what logs to forward, based on criteria like log severity or threat category. Predefined log filters are settings that are built-in to the log forwarding app, and they vary based on the vendor from which you want to forward logs—the firewall, Traps, Cortex XDR - Analytics, and Cortex XDR - Investigation & Response. You can Add or Adjust a Log Filter at any time. After you choose to use predefined filters, you'll see the filters supported for the selected log vendor and log type:

You can also create Custom Log Filters to forward logs based on all possible log fields and values.

Custom Log Filters

Custom filters give you the flexibility to forward logs based on any log field. Use the following operators to build a custom filter:

- And, or (for nested queries)
- Contains, not_contains (strings)
- Eq, geq, leq, gt, lt, neq (strings and integers)
- In, not in (for IP address fields)
For the fields that you can use to build a custom filter, depending on the log source, see:

- **Firewall**: [PAN-OS 9.0 Syslog Field Descriptions](#)
- **Traps**: [Traps log field descriptions](#)
- **Cortex XDR**: For Cortex XDR alerts, you can use these fields to build a custom filter. Custom forwarding filters are not supported for Cortex XDR - Analytics alerts.

## Log Forwarding Filters for Firewall Logs

Here are some examples of custom filters that you can build to forward firewalls logs. See the [PAN-OS 9.0 Syslog Field Descriptions](#) for a full list of the fields on which you can base log forwarding. Predefined log forwarding filters for firewall logs are also built-in to the Log Forwarding app, and vary based on log type.

<table>
<thead>
<tr>
<th>Example</th>
<th>Log Type</th>
<th>Custom Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP logs generated at the start of a session</td>
<td>Traffic</td>
<td>(subtype eq start) and (proto eq tcp)</td>
</tr>
<tr>
<td>Logs for all virtual systems except vsys1</td>
<td>Traffic</td>
<td>(vsys neq vsys1)</td>
</tr>
<tr>
<td>Logs generated when the firewall closed a session because it detected a threat</td>
<td>Traffic</td>
<td>(session_end_reason eq threat)</td>
</tr>
<tr>
<td>Logs with source port 456 and where the destination is not port 45</td>
<td>Traffic</td>
<td>(sport eq 456) and (dport neq 45)</td>
</tr>
<tr>
<td>All logs generated after the start of a session</td>
<td>Traffic</td>
<td>(subtype neq start)</td>
</tr>
<tr>
<td>Logs matching security policy rules that include the word &quot;Inbound&quot;</td>
<td>Traffic</td>
<td>(rule contains 'Inbound')</td>
</tr>
<tr>
<td>Logs for which the application is DNS and the destination is not port 53</td>
<td>Traffic</td>
<td>(app eq dns) and (dport neq 53)</td>
</tr>
<tr>
<td>All logs where the action is not “allow”</td>
<td>Traffic</td>
<td>(action neq allow)</td>
</tr>
<tr>
<td>Threat logs that have a severity of medium or higher (omit logs that are of information or low severity)</td>
<td>Threat</td>
<td>(severity geq medium)</td>
</tr>
<tr>
<td>System logs that have a severity other than “informational”</td>
<td>System</td>
<td>(severity neq informational)</td>
</tr>
</tbody>
</table>
Log Forwarding Filters for Traps Logs

Here are some examples of custom filters that you can build to forward Traps logs. See the Traps log field descriptions for a full list of the fields on which you can base log forwarding. Predefined log forwarding filters for Traps logs are also built-in to the Log Forwarding app, and vary based on log type.

<table>
<thead>
<tr>
<th>Example</th>
<th>Log Type</th>
<th>Custom Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>All WildFire logs that are not benign</td>
<td>WildFire</td>
<td>(category neq benign)</td>
</tr>
</tbody>
</table>

### Log Forwarding Filters for Cortex XDR Alerts

The Cortex XDR app can send logs to Cortex Data Lake. You can then use the Log Forwarding app to send the logs stored in Cortex Data Lake to a Syslog or email destination. If you want to forward a subset of Cortex XDR alert logs (instead of all logs), you can use log forwarding filters to specify which logs you want to send.

#### Cortex XDR - Analytics Alerts

When you enable forwarding for Cortex XDR - Analytics alerts, the Log Forwarding app sends all Cortex XDR Analytics alert logs to the Syslog or email destination you specify (learn more about log fields and formats). Log forwarding filters are not available for Cortex XDR - Analytics alerts.

#### Cortex XDR Alerts

The Log Forwarding app provides both predefined and custom log forwarding filters for (non-Analytics) Cortex XDR alerts. Predefined Log Filters are built-in to the Log Forwarding app, so that you can easily start forwarding Cortex XDR alerts based on severity, alert source (a BIOC or IOC rule), and alert category.
• **Severity**—The alert severity levels you can filter on are informational, low, medium, high, and unknown.

• **Alert Source**—This is the type of Cortex XDR - Investigation and Response alert. BIOCs identify specific network, process, file, or registry activity that indicates a threat; IOCs are known artifacts—SHA256 hashes, IP addresses, domains, file names—that are considered malicious or suspicious.

• **Alert Category**—The alert categories listed are different for BIOC and IOC alerts, and allow you to further narrow the types of logs you want to forward based on the detected threat artifact or behavior. BIOC alert categories include exfiltration, credential access, and tampering; IOC alert categories include hash, file name, IP address, and domain name.

Additionally, you can build custom log filters to forward logs based on any Cortex XDR alert log fields. For more details on custom filters, including supported operators, see Custom Log Filters. Here are some examples of custom filters for Cortex XDR alerts.

<table>
<thead>
<tr>
<th>Example</th>
<th>Log Type</th>
<th>Custom Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>High severity BIOC and IOC alerts</td>
<td>Alert</td>
<td>(severity eq SEV_040_HIGH)</td>
</tr>
<tr>
<td>BIOC alerts for unusual credential usage</td>
<td>Alert</td>
<td>(alert_category eq CREDENTIAL_ACCESS)</td>
</tr>
<tr>
<td>Alerts of all severities except for informational alerts</td>
<td>Alert</td>
<td>(severity neq SEV_010_INFO)</td>
</tr>
<tr>
<td>High severity IOC alerts for suspicious file names or SHA-256 hashes</td>
<td>Alert</td>
<td>(severity eq SEV_040_HIGH) and ((alert_category eq FILENAME) or (alert_category eq HASH))</td>
</tr>
</tbody>
</table>
List of Trusted Certificates for the Log Forwarding App

List of trusted CA certificates on the Log Forwarding app:

- Issuer: CN=DigiCert Assured ID Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US
- Issuer: CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB
- Issuer: EMAILADDRESS=premium-server@thawte.com, CN=Thawte Premium Server CA, OU=Certification Services Division, O=Thawte Consulting cc, L=Cape Town, ST=Western Cape, C=ZA
- Issuer: CN=SwissSign Platinum CA - G2, O=SwissSign AG, C=CH
- Issuer: CN=SwissSign Silver CA - G2, O=SwissSign AG, C=CH
- Issuer: CN=DST Root CA X3, O=Digital Signature Trust Co.
- Issuer: CN=DST Root CA X3, O=Digital Signature Trust Co.
- Issuer: CN=Equifax Secure eBusiness CA-1, O=Equifax Secure Inc., C=US
- Issuer: CN=SecureTrust CA, O=SecureTrust Corporation, C=US
- Issuer: CN=DigiCert Assured ID Root G3, OU=www.digicert.com, O=DigiCert Inc, C=US
- Issuer: CN=UTN-USERFirst-Client Authentication and Email, OU=http://www.usertrust.com, O=The USERTRUST Network, L=Salt Lake City, ST=UT, C=US
- Issuer: CN=DigiCert Assured ID Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US
- Issuer: CN=IdenTrust Public Sector Root CA 1, O=IdenTrust, C=US
- Issuer: CN=AffirmTrust Networking, O=AffirmTrust, C=US
- Issuer: CN=Entrust Root Certification Authority, OU="(c) 2006 Entrust, Inc.", OU=www.entrust.net/CPS is incorporated by reference, O="Entrust, Inc.", C=US
- Issuer: CN=UTN-USERFirst-Hardware, OU=http://www.usertrust.com, O=The USERTRUST Network, L=Salt Lake City, ST=UT, C=US
- Issuer: CN=GlobalSign, O=GlobalSign, OU=GlobalSign ECC Root CA - R5
- Issuer: CN=GlobalSign, O=GlobalSign, OU=GlobalSign ECC Root CA - R4
- Issuer: CN=Certum CA, O=Unizeto Sp. z o.o., C=PL
- Issuer: CN=AddTrust Class 1 CA Root, OU=AddTrust TTP Network, O=AddTrust AB, C=SE
- Issuer: CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US
- Issuer: CN=Equifax Secure Certificate Authority, O=Equifax, C=US
- Issuer: CN=QuoVadis Root CA 3, O=QuoVadis Limited, C=BM
- Issuer: CN=QuoVadis Root CA 2, O=QuoVadis Limited, C=BM
- Issuer: CN=Swisscom Root CA 2, OU=Digital Certificate Services, O=Swisscom, C=CH
- Issuer: CN=DigiCert Global Root G3, OU=www.digicert.com, O=DigiCert Inc, C=US
- Issuer: CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US
- Issuer: CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US
- Issuer: CN=Equifax Secure Global eBusiness CA-1, O=Equifax Secure Inc., C=US
- Issuer: CN=GeoTrust Universal CA, O=GeoTrust Inc., C=US
- Issuer: CN=Class 3 Public Primary Certification Authority, O="VeriSign, Inc.", C=US
- Issuer: CN=thawte Primary Root CA - G3, OU="(c) 2008 thawte, Inc. - For authorized use only", OU=Certification Services Division, O="thawte, Inc.", C=US
- Issuer: CN=thawte Primary Root CA - G2, OU="(c) 2007 thawte, Inc. - For authorized use only", O="thawte, Inc.", C=US
- Issuer: CN=Deutsche Telekom Root CA 2, OU=T-TeleSec Trust Center, O=Deutsche Telekom AG, C=DE
• Issuer: CN=Swisscom Root EV CA 2, OU=Digital Certificate Services, O=Swisscom, C=CH
• IssuerDomain:CertificatePolicyId: [2.16.756.1.83.2.2]
• Issuer: CN=Thawte Timestamping CA, OU=Thawte Certification, O=Thawte, L=Durbanville, ST=Western Cape, C=ZA
• Issuer: CN=QuoVadis Root Certification Authority, OU=Root Certification Authority, O=QuoVadis Limited, C=BM
• Issuer: CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US
• Issuer: CN=AffirmTrust Premium ECC, O=AffirmTrust, C=US
• Issuer: CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB
• Issuer: CN=KEYNECTIS ROOT CA, OU=ROOT, O=KEYNECTIS, C=FR
• Issuer: CN=AddTrust Qualified CA Root, OU=AddTrust TTP Network, O=AddTrust AB, C=SE
• Issuer: CN=America Online Root Certification Authority 2, O=America Online Inc., C=US
• Issuer: CN=America Online Root Certification Authority 1, O=America Online Inc., C=US
• Issuer: CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE
• Issuer: CN=VeriSign Class 2 Public Primary Certification Authority - G3, OU="(c) 1999 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US
• Issuer: CN=LuxTrust Global Root, O=LuxTrust s.a., C=LU
• Issuer: OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 2 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US
• Issuer: CN=QuoVadis Root CA 3 G3, O=QuoVadis Limited, C=BM
• Issuer: CN=GeoTrust Primary Certification Authority - G3, OU=(c) 2008 GeoTrust Inc. - For authorized use only, O=GeoTrust Inc., C=US
• Issuer: CN=GeoTrust Primary Certification Authority - G2, OU=(c) 2007 GeoTrust Inc. - For authorized use only, O=GeoTrust Inc., C=US
• Issuer: CN=SwissSign Gold CA - G2, O=SwissSign AG, C=CH
• Issuer: CN=Entrust.net Certification Authority (2048), OU=(c) 1999 Entrust.net Limited, OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.), O=Entrust.net
• Issuer: OU=ePKI Root Certification Authority, O="Chunghwa Telecom Co., Ltd.", C=TW
• Issuer: CN=QuoVadis Root CA 2 G3, O=QuoVadis Limited, C=BM
• Issuer: CN=Global Chambersign Root - 2008, O=AC Camerfirma S.A., SERIALNUMBER=A82743287, L=Madrid (see current address at www.camerfirma.com/address), C=EU
• Issuer: CN=QuoVadis Root CA 1 G3, O=QuoVadis Limited, C=BM
• Issuer: CN=Chambers of Commerce Root - 2008, O=AC Camerfirma S.A., SERIALNUMBER=A82743287, L=Madrid (see current address at www.camerfirma.com/address), C=EU
• Issuer: CN=USERTrust ECC Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US
• Issuer: OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US
• Issuer: CN=IdenTrust Commercial Root CA 1, O=IdenTrust, C=US
• Issuer: CN=AffirmTrust Premium, O=AffirmTrust, C=US
• Issuer: CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US
• Issuer: CN=VeriSign Class 1 Public Primary Certification Authority - G3, OU="(c) 1999 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US
• Issuer: OU=Security Communication EV RootCA1, O="SECOM Trust Systems CO.,LTD.", C=JP
• Issuer: CN=D-TRUST Root Class 3 CA 2 EV 2009, O=D-Trust GmbH, C=DE
• Issuer: OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 1 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US
• Issuer: CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB
• Issuer: CN=Go Daddy Root Certificate Authority - G2, O=“GoDaddy.com, Inc.”, L=Scottsdale, ST=Arizona, C=US