
CA Certificates

A **CA certificate** allows you to control access to realms, roles, and resource policies based on certificates or certificate attributes. For example, you may specify that users must present a valid client-side certificate with the DN attribute set to "yourcompany.com" in order to access the "Users" authentication realm. For information about realm, role, and resource policy certificate checks, see "Certificate restrictions" in Appendix B of the *IVE Administration Guide*.

To use CA certificates, you must install and enable the proper certificates on the IVE as well as install the corresponding client-side certificates in the Web browsers of your end-users. When validating users with CA certificates, the IVE checks that the certificate is not expired or corrupt and that the certificate is signed by a CA that is recognized by the IVE. If the CA certificate is chained (described below) the IVE also follows the chain of issuers until it reaches the root CA, checking the validity of each issuer as it goes.

The IVE also supports using the following additional features with CA certificates:

- **Certificate servers**

A certificate server allows you to authenticate IVE users based solely on their certificate attributes rather than authenticating users against a standard authentication server (such as LDAP or SiteMinder) as well as requiring specific certificates or certificate attributes. For more information, see the "Certificate servers" on page 2.

- **Certificate hierarchies**

Within a certificate hierarchy, one or more subordinate certificates (called intermediate certificates) are branched off of a root certificate. Each intermediate certificate (also called a chained certificate) is signed by the root CA and handles requests for a part of the root CA's domain. For example, you may create a root certificate that handles all requests to the "yourcompany.com" domain and then branch off intermediate certificates that handle requests to "partners.yourcompany.com" and "employees.yourcompany.com." You may also create trust relationships across various certificate hierarchies. For more information, see "Certificate hierarchies" on page 2.

- **Certificate revocation lists**

Certificate revocation is a mechanism by which a CA invalidates a certificate before its expiration date. A certificate revocation list (CRL) is a list of revoked certificates published by a CA. Within CRLs, each entry contains the serial number of the revoked certificate, the date that the certificate was revoked, and the reason that the certificate was revoked. The CA may invalidate a certificate for various reasons such as the

employee to whom the certificate is issued has left the company, the certificate's private key is compromised, or the client-side certificate is lost or stolen. Once the CA revokes a certificate, the IVE can appropriately deny access to users who present a revoked certificate. For more information, see "Certificate revocation lists" on page 3.

Certificate servers

The certificate server feature allows users to authenticate based on attributes contained in client-side certificates. You may use certificate server by itself or in conjunction with another server to authenticate users and map them to roles.

For example, you may choose to authenticate users solely based on their certificate attributes. If the IVE determines that the user's certificate is valid, it signs the user in based on the certificate attributes you specify and does not prompt the user to enter a username or password.

Or, you may choose to authenticate users by passing their client-side certificate attributes to a second authentication server (such as LDAP). In this scenario, the certificate server first determines if the user's certificate is valid. If it is, the certificate server passes selected attributes to an LDAP server that maintains a CRL. If the user's certificate has been revoked (because he left the company or changed job titles), the LDAP server returns a "bad" status to the IVE and the IVE denies the user access. If the LDAP server returns a "good" status, the IVE maps the user to a role based on a value returned by the LDAP server.

For configuration instructions, see "Configuring a certificate server instance" on page 10.

Certificate hierarchies

Within a certificate hierarchy, one or more intermediate certificates are branched off of a single root certificate. The root certificate is issued by a root certificate authority (CA), is self-signed, and acts as the master authority for the entire domain. Each intermediate certificate is signed by an intermediate CA, is trusted by the certificate above it in the chain, and validates users in a sub-section of the domain.

To enable authentication in a chained certificate environment, you must install the appropriate client-side certificates in each user's Web browser and then upload the corresponding server-side certificates to the IVE through the **System > Configuration > Certificates > CA Certificates**

page of the Web console¹. When uploading the certificate chain to the IVE, you must use one of the following methods:

- **Import the entire certificate chain at once**

When installing a chain of certificates contained in a single file, the IVE imports the root certificate and any sub-certificates whose parents are in the file or on the IVE. You can include certificates in any order in the import file.

- **Import the certificates one at a time in descending order**

When installing a chain of certificates contained in multiple files, the IVE requires that you install the root certificate first, and then install the remaining chained certificates in descending order.

When you install chained certificates using one of these methods, the IVE automatically chains the certificates together in the correct order and displays them hierarchically in the Web console.

Note: If you install multiple certificates in a user's Web browser, the browser prompts the user to choose which certificate to use whenever he signs into the IVE.

For configuration instructions, see "Upload CA certificates to the IVE" on page 5.

Certificate revocation lists

A **certificate revocation list (CRL)** is a mechanism for maintaining access to servers. As the name implies, a CRL is a list of list of revoked certificates published by a CA or delegated CRL issuer. The IVE supports two types of CRLs:

- **Base CRL**

When a CA publishes a base CRL for a company, it includes all of the company's revoked certificates in a single, unified list.

- **Partitioned CRLs**

When a CA publishes a partitioned CRL for a company, it separates the list into groups of users. Enterprises with large numbers of users frequently use partitioned CRLs for load-balancing.

The IVE knows which CRL to use by checking the client's certificate. (When issuing a certificate, the CA includes CRL information for the certificate in

1. With a Baseline license, you cannot install a chain whose certificates are issued by different CAs. The CA that signs the lowest-level certificate in the chain must also sign all other certificates in the chain (except the root, which is self-signed.)

the certificate itself.) To ensure that it is receiving the most up-to-date CRL information, the IVE periodically contacts a CRL distribution point to get an updated list of revoked certificates. A **CRL distribution point (CDP)** is a location on an LDAP directory server or Web server where a CA publishes CRLs. The IVE downloads CRL from the CDP at the interval specified in the CRL, at the interval that you specify during CRL configuration, and when you choose to manually download the CRL.

Although CAs include CRL information in client-side certificates, they do not always includes CDP information as well. A CA may use any of the following methods to notify the IVE of a certificate's CDP location:

- **Specify the CDP(s) in the CA certificate**

When the CA issues a CA certificate, it includes an attribute specifying the location of the CDP(s) that the IVE should contact. If more than one CDP is specified, the IVE chooses the first one listed in the certificate and then fails over to subsequent CDPs if necessary.

- **Specify the CDP(s) in the client certificates**

When the CA issues client-side certificates, it includes an attribute specifying the location of the CDP(s) that the IVE should contact. If more than one CDP is specified, the IVE chooses the first one listed in the certificate and then fails over to subsequent CDPs if necessary. (Commonly used with partitioned CRLs.)

Note: If you choose this method, the user receives an error the first time he tries to sign into the IVE because no CRL information is available. Once the IVE recognizes the client's certificate and extracts the CRL location, it can start downloading the CRL and subsequently validate the user's certificate. In order to successfully sign into the IVE, the user must try to reconnect after a few seconds.

- **Require the administrator to manually enter the CDP location**

If the CA does not include the CDP location in the client or CA certificates, you must manually specify how to download the entire CRL object when configuring the IVE. You may specify a primary and backup CDP. (Manually entering the CDP location provides the greatest flexibility because you do not need to reissue certificates if you change your CDP location.)

The IVE checks the user's certificate against the appropriate CRL during authentication. If it determines that the user's certificate is valid, the IVE caches the CRL attributes and applies them if necessary during role and resource policy checks. If it determines that the user's certificate is invalid,

if it cannot contact the appropriate CRL, or if the CRL is expired, the IVE denies the user access.

Important: The IVE only supports CRLs that are in a PEM or DER format and that are signed by the CA for which the revocations apply. Also note that the IVE only saves the first CRL in a PEM file.

For configuration instructions, see “Enable CRL checking” on page 7.

Configuring the Certificates > CA Certificate tab

Use the **System > Configuration > Certificates > CA Certificate** tab to import CA certificates and configure CA certificate options. The IVE supports all standard X.509 certificates.

Tasks in this section include:

Upload CA certificates to the IVE	5
Renew a CA certificate.....	6
Enable CRL checking.....	7
View CA certificate details.....	8

Upload CA certificates to the IVE

If you require users to provide a client-side certificate to sign in to the IVE, you must upload the corresponding CA certificate into the IVE. The IVE uses the uploaded certificate to verify that the browser-submitted certificate is valid.

Important:

- When using client-side certificates, we strongly recommend that you train your users to close their Web browsers after signing out of the IVE. If they do not, other users may be able to use their open browser sessions to access certificate-protected resources on the IVE without reauthentication. (After loading a client-side certificate, both Internet Explorer and Netscape cache the certificate’s credentials and private key. The browsers keep this information cached until the user closes the browser (or in some cases, until the user reboots the workstation). For details, see: <http://support.microsoft.com/?kbid=290345>.) To remind users to close their browsers, you may modify the sign out message in the **System > Signing In > Sign-in Pages** tab.
- Uploading a CA certificate to the IVE does not enable client-side SSL authentication. You must either use a certificate server or enable

Browsing to SSL Sites option in the **System > Configuration > Security > Security Options** tab of the Web console in order to enable client-side SSL authentication.

- When uploading a certificate chain to the IVE, you must either install the certificates one at a time in descending order starting with the root certificate (DER or PEM files), or you must upload a single file to the IVE that contains the entire certificate chain (PEM files only). By using one of these methods, you ensure that the IVE can link the certificates together in the correct order.

To upload CA certificates to the IVE:

1. Install a client-side certificate through the user's browser. For help, see the instructions provided with the browser.
2. In the Web console, choose **System > Configuration > Certificates > CA Certificates**.
3. Click **Import CA Certificate**.
4. Browse to the CA certificate that you want to upload to the IVE and click **Import Certificate**.
5. Determine which realms should use the certificate to authenticate users and then enable the certificate for those realms using settings in the **Users > Authentication > [Realm] > Authentication Policy > Certificate** tab.
6. Use the instructions in the *IVE Administration Guide* to specify X.509 Distinguished Name (DN) attributes that users must present for authentication, role access, or resource policy access or to enable certificate authentication for administrator realms in addition to user realms (optional).

Renew a CA certificate

In order to renew a CA certificate, your CA must issue you a new certificate that uses the same private key as your existing certificate and then upload the new certificate to the IVE.

To import a renewed CA certificate into the IVE:

1. In the Web console, choose **System > Configuration > Certificates > CA Certificate**.
2. Click the link that corresponds to the certificate that you want to renew.
3. Click **Renew Certificate**.
4. Browse to the renewed CA certificate that you want to upload to the IVE and click **Import Certificate**.

Enable CRL checking

You can enable and periodically download certificate revocation lists (CRL) from CRL distribution points (CDPs) in order to verify the ongoing validity of client-side certificates.

To enable CRL checking:

1. In the Web console, choose **System > Configuration > Certificates > CA Certificate**.
2. Click the link that corresponds to the certificate for which you want to enable CRL checking.
3. Click **CRL Checking Options**.
4. Under **CRL Distribution Points**, specify where the IVE should find access information for the CDP. Options include:

- **No CDP (no CRL Checking)**

When you select this option, the IVE does not check CRLs issued by the CA, so you do not need to enter any parameters to access the CDP that issued the CRL.

- **CDP(s) specified in the CA Certificate**

When you select this option, the IVE checks the CRL distribution point attribute in the certificate and displays the URIs of the CDPs that it finds in the **CRL Checking Options** page. If the CA certificate does not include all of the information required to access the CDP, specify the additional required information:

- **CDP Server:** Enter the location of the CDP server. When using LDAP protocol, enter the IP address and port (for example, ldap.domain.com:6000). When using HTTP protocol, enter the complete path to the CRL object (for example, https://domain.com/CertEnroll/CompanyName%20CA%20Server.crl).
- **CRL Attribute:** Enter the attribute on the object that contains the CRL (for example, CertificateRevocationList).
- **Admin DN, Password:** (LDAP only) If the CDP server does not allow anonymous searches of the CRL, enter the admin DN and password that are required to authenticate into the CDP server.

- **CDP(s) specified in client certificates**

When you select this option, the IVE checks the CRL distribution point attribute in the certificate and displays the URIs of the CDPs that it finds in the **CRL Checking Options** page. If the client certificate does not include all of the information required to access the CDP, specify the additional required information:

- **CDP Server:** Enter the location of the CDP server. When using LDAP protocol, enter the IP address and port (for example,

ldap.domain.com:6000). When using HTTP protocol, enter the complete path to the CRL object (for example, `https://domain.com/CertEnroll/CompanyName%20CA%20Server.crl`).

- **CRL Attribute:** Enter the attribute on the object that contains the CRL (for example, CertificateRevocationList).
- **Admin DN, Password:** (LDAP only) If the CDP server does not allow anonymous searches of the CRL, enter the admin DN and password that are required to authenticate into the CDP server.

Manually configured CDP

When you select this option, the IVE accesses the CDP that you specify. Enter the URL of the primary CDP and optionally of a backup CDP. For an LDAP server, use the syntax:

ldap://<Server>/BaseDN?attributes?Scope?Filter. For a Web server, enter the complete path to the CRL object. For example: `https://domain.com/CertEnroll/CompanyName%20CA%20Server.crl`

Additionally, if the CDP server does not allow anonymous searches of the CRL, enter the admin DN and password that are required to authenticate into the CDP server.

Note: If you choose to download CDPs using one method and then select a different method, the IVE deletes any CDPs from disk that were downloaded using the previous method.

5. In the **CRL Download Frequency** field, specify how often the IVE should download the CRL from the CDP.
6. If you want to check the validity of your CA certificate (in addition to client-side certificates) against the CRL specified in the previous steps, select **Verify CA certificate** on the CA Certificate page.

Important: When you choose to verify an intermediate certificate, make sure that CRLs are available for all of the CA certificates that are above the intermediate certificate in the chain. When verifying a CA certificate, the IVE also verifies all issuing CAs above the certificate in the chain.

7. Click **Update Now** to manually download the CRL from the CDP (optional).
8. Click **Save Changes**. The IVE downloads the CRL using the method you specified (if applicable) and displays CRL checking details (described in the following section).

View CA certificate details

You can view a variety of details about each of the CA certificates installed on the IVE.

To view CA certificate details:

1. In the Web console, choose **System > Configuration > Certificates > CA Certificate**.
2. Click the certificate that you want to view.
3. Under **Certificate**, use the arrow next to the following field names to view certificate details:
 - **Issued To**
Name and attributes of the entity to whom the certificate is issued.
 - **Issued By**
Name and attributes of the entity that issued the certificate. Note that the value of this field should either match the **Issued To** field (for root certificates) or the **Issued To** field of the next certificate up in the chain (for intermediate certificates).
 - **Valid Dates**
Time range that the certificate is valid. If your certificate is expired, see the instructions in “Renew a CA certificate” on page 6.
 - **Details**
Includes various certificate details, including its version, serial number, signature algorithm, CRL distribution points, public key algorithm type, and the public key. Note that although the IVE may display a CRL distribution point in the **Details** field, it does not check the CDP unless you enable it. For more information, see “Enable CRL checking” on page 7.
4. Under **CRL checking for client certificates**, view details about the CRL(s) that are enabled for this certificate:
 - **Enable**
Displays a check mark if CRL checking is enabled for the certificate.
 - **CRL Distribution Points**
Location of the CRL distribution point against which the certificate is validated. This field also indicates whether or not the IVE successfully downloaded the CRL from the CDP.
 - **Status**
Indicates the status of the CRL (OK, No CRL, Expired), the CRL size, and the number of revocations contained in the CRL.
 - **Last Updated**
Indicates the last time the IVE downloaded a CRL from the specified CRL distribution point. Also contains a link that allows you to save the IVE's current version of the CRL.
 - **Next Update**
Indicates the next time the IVE is scheduled to download a CRL from

the specified CRL distribution point. Note that a download interval is specified both in the CRL and in the IVE CRL configuration page—the value shown here is the lesser of those two values.

Configuring a certificate server instance

Define a certificate server configuration

When defining a certificate server on the IVE, you must perform the following steps:

1. Use settings in the **System > Configuration > Certificates > CA Certificates** tab to import the CA certificate used to sign the client-side certificates.
2. Create a certificate server instance:
 1. Navigate to **System > Signing In > Servers**.
 2. Select **Certificate Server** from the **New** list, and then click **New Server**.
 3. Specify a name to identify the server instance. Note that if you change the name of an existing server, the IVE creates a new certificate instance with the new name and retains the old server as well.
 4. In the **User Name Template** field, specify how the IVE should construct a username. You may use any combination of certificate variables contained in angle brackets and plain text. For a list of certificate variables, see “System variables and examples” in Appendix C of the IVE Administration Guide.

Note: If you choose a certificate attribute with more than one value, the IVE uses the first matched value. For example, if you enter <certDN. OU> and the user has two values for the attribute (ou=management, ou=sales), the IVE uses the “management” value.

5. Click **Save Changes**. If you are creating the server instance for the first time, the **Settings** and **Users** tabs appear.

Note: For information about monitoring and deleting the sessions of users who are currently signed in through the server, see “View and delete user sessions” on page 212.

3. If you want to verify certificate attributes against an LDAP server, use settings in the **System > Signing In > Servers** page to create an LDAP server instance. Note that you must use the **Finding user entries** section in the LDAP configuration page to retrieve the user-specific attributes that you want verify through the certificate.

4. Use settings in the **Users > Authentication > Authentication > General** tab or **Administrators > Authentication > General** tab to specify which realms should use the certificate server to authenticate users. (You may also use settings in these tabs to specify realms that should use an LDAP server to verify certificate attributes.)
5. Use settings in the **System > Signing In > Sign-in Policies** page to associate the realms configured in the previous step with individual sign-in URLs.
6. If you want to restrict users' access to realms, roles, or resource policies based on individual certificate attributes, use the settings described in "Certificate restrictions" in Appendix B of the *IVE Administration Guide*.