Enterprise Certificate Console

Simplified Control for Digital Certificates from the Cloud
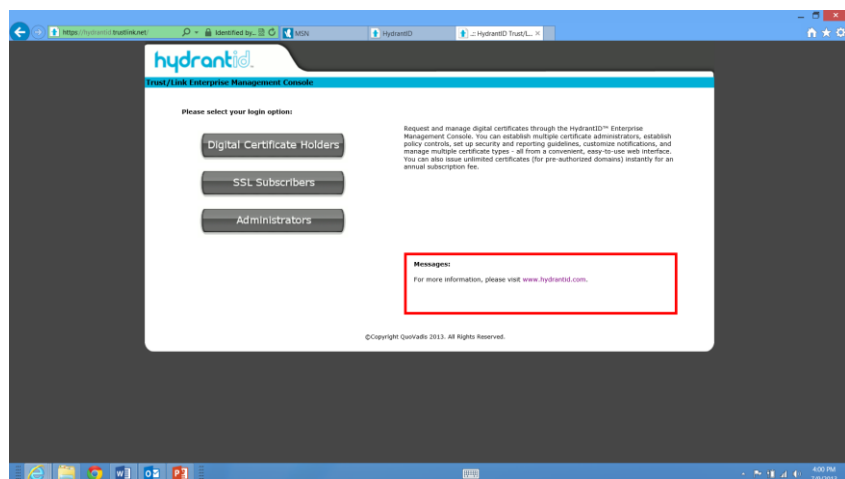
HydrantID Enterprise Management Console

HydrantID's HydrantSSL Enterprise service and HydrantCloud Managed PKI services are all delivered through our HydrantID Enterprise Management Console.

- **HydrantSSL Enterprise Service:** If your organization requires multiple SSL certificates and multiple administrators with granular management and audit controls, then our HydrantSSL Enterprise service has you covered. With real-time issuance of SSL Certificates for pre authorized domains - Our HydrantID Management Console makes taking control of your SSL certificates simple and easy – on demand from the cloud.
- *HydrantCloud Managed PKI (Power and dedicated services):* Get all of your organizational PKI certificate needs from the cloud. Whether you take advantage of our streamlined pre-configured CA service (Power) or leverage our highly customizable service (Dedicated) - Its all delivered, on demand and from the cloud through our HydrantID Enterprise Management Console.

Organizations often struggle to control their use of Digital Certificates across their variety of business units and locations. HydrantID's Enterprise Management Console allows organizations to easily issue Certificates on demand, maintaining central oversight while providing flexibility for different groups to define their own request and approval processes.

The HydrantID Enterprise Management Console is a cloud-based control panel that allows customers to manage the full lifecycle of their Digital Certificates, from signup to revocation or renewal. Leveraging HydrantID's highly accredited certification authority operations, The HydrantID Enterprise Management Console

allows Organizations to easily obtain Certificates, on demand in real time.

The HydrantID Enterprise Management Console provides great flexibility for Organizations, whether you simply require SSL for your websites, or have multiple PKI projects in separate business units using different types of Digital Certificates, including SSL, S/mime, client certificates, utility/device certificates.

With delegated administration, The HydrantID Enterprise Management Console allows you to tailor custom workflows, templates, and emails for each business unit or group in the account. This flexibility provides a powerful tool to meet local business needs, while maintaining central control for cost and reporting reasons.

All Enterprise Management Console components are hosted and managed through HydrantID. Administrators and Subscribers are not required to install any additional software on their computers. The HydrantID Enterprise Management Console is a .NET Framework v3.5 web-based

application.   In addition, The HydrantID Enterprise Management Console is UTF8-ready for use of international character sets.

System Structure

The HydrantID Enterprise Management Console has three major components for your users:

- *Administrator Control Panel:* The HydrantID Enterprise Management control panel, with certificate based two-factor access, provides granular administration of your groups, users, and other settings. It also allows your Administrators to manage Certificates through their entire lifecycle and to use the system's extensive reporting tools.

- *Subscriber Portal:* Your Administrators may invite new certificate Subscribers to work with specific Organizations within the Account. Organizations may be added or removed from a Subscriber at any time. Thereafter, the Subscriber may request new Certificates and manage their existing Certificates from one password login. A variant of this portal is used for End User or client Certificate Holders to pickup and manage their Certificates.

- *API:* An optional secure Web Services component allows Organizations to build or use their own Web interfaces for Certificate request and revocation, interacting with The HydrantID Enterprise Management Console for the approval process and Certificate production.

Flexible Administration

The HydrantID Enterprise Management Console is highly scalable and provides extensive options to tailor the Certificate types and administrative workflow needed for your different business units:

- *System:* HydrantID administrates the HydrantID Enterprise Management Console system, to set up Accounts, and to make system configurations. HydrantID has access to system-wide reporting capabilities but does not process individual Certificate requests.

- *Account:* Each customer organization acts as an Account in The HydrantID Enterprise Management Console, allowing their permissions and activity to be segregated from others. Each Account has a Primary Administrator from whom authority is delegated to all other users (Administrators and Subscribers) within that Account. The HydrantID Enterprise Management Console provides the Primary Administrator with extensive audit trails both by Certificate and by user.

- *Organization:* The Account may be divided into groups/organizations, and each Organization may have a different mix of
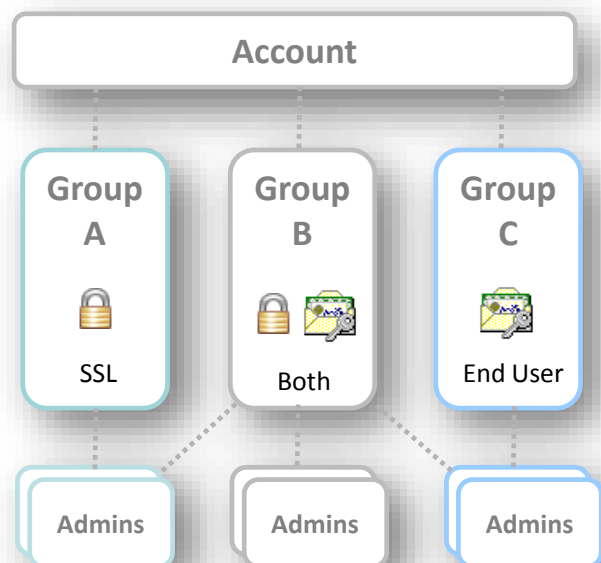
Certificate types and workflows to allow segregation between the departments/companies served by that Account.

Administrators and Subscribers may be assigned to multiple Organizations within the Account. If desired, The HydrantID Enterprise Management Console may be configured to require "second authorization" by Administrators before Certificate approvals and revocations are processed.

Administrator Roles

The HydrantID Enterprise Management Console provides granularity in the permissions assigned to different Administrators, providing great flexibility in system operations ranging from a flat structure for small projects to diverse issuance workflows for enterprise work.

Every Account has a Primary Administrator, who is the key contact for HydrantID when validating domains and other Certificate details. The Primary Administrator has all permissions across all Organizations in the Account. For small implementations, you may choose to operate with only this single Primary Administrator.

For larger Accounts, the Primary Administrator may choose to create unlimited additional Administrators with different permission levels:

Permission	SSL	End User
Approve Certificate Requests	✗	✗
Manage Invitations		✗
Manage Subscribers	✗	
Modify Certificate Request Template	✗	
Modify Email Templates	✗	✗
Modify Invitation Templates		✗
Retrieve Certificates From Archive		✗
Revoke Certificates	✗	✗
Search/Reports	✗	✗

- Grant "all Organizations, all permissions" or assign to specific groups
- Assign by Certificate type
- Restrict to specific permission

This allows Certificate processing to be delegated to the corresponding business unit or subsidiary company, as well as for work balancing or separation of duties.

	This Month (April)	This Year (2010)
Certificates Issued:	0	0
Certificates Revoked:	0	0
		As of today
Certificates Expiring in the next 30 days:		0
Certificate Requests Pending Approval:		0
Certificates Requests Pending Authorisation:		0
Certificates Not Yet Downloaded:		0
Certificate Revocation Requests Pending Authorisation:		0

The Administrators' *My Profile page* provides an overview of groups and permissions assigned to them.

When they log in to The HydrantID Enterprise Management Console, the Administrators' landing page provides a Dashboard with links to all pending activity requiring their attention.

HydrantID Roles

HydrantID Managers administrate the overall HydrantID Enterprise Management Console system, including setting up and managing Accounts and their Administrators.

HydrantID also oversees the validation of all Organizations and Domains requested by Accounts, and their enablement in the system. In some cases, subject to additional contractual requirements, HydrantID may delegate aspects of this validation to specific Account Administrators. Those requirements typically include specific training, recordkeeping, and audit obligations related to acting as a Registration Authority in the HydrantID PKI.

HydrantID provides support for the HydrantID Enterprise Management Console application, and assists Subscribers/Certificate Holders in troubleshooting their Certificate installations. HydrantID Support does not intervene in the approval of individual Certificate Requests. This processing must be performed by the delegated Administrators for the corresponding Account.

Custom Notifications

Administrators may tailor the Certificate Request forms used by The HydrantID Enterprise Management Console, including custom fields to collect internal information, such as internal project codes, that are not included in the certificate itself.

The HydrantID Enterprise Management Console provides a variety of notification emails that are used to alert Administrators and Subscribers/Certificate Holders when orders require their attention. The text of the default emails may be customised by the Primary Administrator for use across the Account, or tailored for each Organization.

Search and Reporting

The HydrantID Enterprise Management Console provides comprehensive search capabilities for Administrators and Subscribers/Certificate Holders to search their assigned populations of pending orders and previously issued Certificates.

In addition, The HydrantID Enterprise Management Console allows Administrators to run "real time" and historical summaries for their assigned populations:

- Certificate Summary (totals of active Certificates and pending requests during a time period)
- Certificate Detail (detailed information of active Certificates and pending requests during a time period)
- Inventory of Valid Certificates at a point in time
- Audit report for specific Certificate order
- Audit reports by Account or by Administrator for a period of time
- Audit reports for notification emails sent by The HydrantID Enterprise Management Console by Account

Certificate Types

The HydrantID Enterprise Management Console is able to provision a wide range of Certificate types, by Organisation within an Account:

SSL		• Business SSL (standard validated) • Business SSL with EV SSL (extended validation) • SAN Certificates (Optional EV) • Wildcard certificates • Variable duration periods
Device & Client certificates		• HydrantID standard Certificate classes, tailored for your use case • Variety of issuance methods (form, CSR, bulk upload) • Custom registration templates with fixed/variable fields • Option for private key archive and recovery • Support for tokens

During early renewals, The HydrantID Enterprise Management Console automatically extends the validity period of the replacement Certificate with the unused duration of the renewed Certificate.

Certificate Processing

The HydrantID Enterprise Management Console may be configured to provide different issuance processes for Certificates:

1. **Invitations**: In default operation, the Administrator uses The HydrantID Enterprise Management Console workflows to communicate with the Subscriber/Certificate Holder and facilitate the Certificate Request and delivery process. Subscribers/Certificate Holders have access to their own portal to manage the Certificate lifecycle, including revocation and renewal.

2. **Generate**: In some cases, the Account may want Administrators themselves to generate Certificates themselves, without a workflow to communicate with remote users. This may be useful when Certificate operations are controlled by a core security team or helpdesk. (If an email address is included in the Certificate, The HydrantID Enterprise Management Console notifies the address even if the generate function is used.)

In addition, to facilitate onboarding to The HydrantID Enterprise Management Console, the service provides an add renewal function for existing Certificates even from other providers.

HydrantSSL Enterprise

With our robust HydrantSSL Enterprise service, HydrantID provides unlimited certificates per domain with real time issuance - on demand form our highly accredited cloud infrastructure. Our HydrantSSL Enterprise service is delivered through our HydrantID Enterprise Management Console.

Under most retail SSL sales channels, your technical contacts are tasked with providing corporate validation details they may know nothing about. With The HydrantID Enterprise Management Consloe's pre-validated templates, your invited Subscribers focus on the technical tasks (CSR submission and Certificate installation) for rapid order processing.

Using The HydrantID Enterprise Management Console, Administrators invite Subscribers to have access to certain organizations and Domains. Once logged in, Subscribers have a dashboard to manage their existing Certificates as well as access simple forms to place new orders.
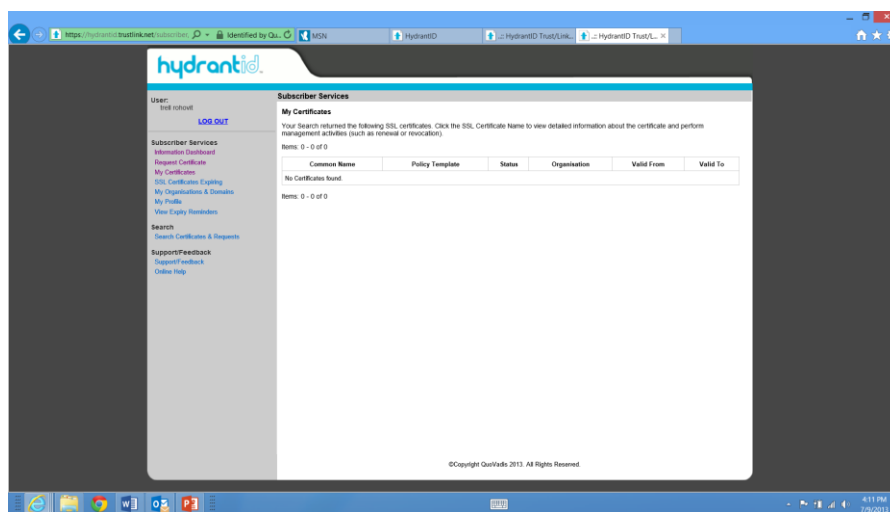
The HydrantID Enterprise Management Console routes incoming orders to the relevant Administrator for processing. Any incoming request with an unapproved Organization or Domain is "parked" until validation is completed.

Administrators may take the following steps before approving or rejecting the Certificate Request.

- Reassign the order to a different Organisation (with its corresponding pre-vetted Certificate template) under their control;
- Change the Certificate type or duration;
- Add or amend the Organization Unit (OU) field;
- Correct the Common Name (CN) of the Certificate, or optionally to insert Domain Components (DC) or SAN fields; and
- Add comments to the Audit trail for the Certificate Request.

Upon approval, The HydrantID Enterprise Management Console alerts the Subscriber by email that their Certificate is ready for pickup from the same Subscriber Services account. Subscribers may download their SSL Certificates in multiple formats used by different server platforms.

The HydrantID Enterprise Management Console also includes options that may be turned on for specific Organizations. These include:

- Second authorization by a specific Administrator may be required before Certificate Requests may be approved or Certificates revoked.

- Alerts may be sent to external users (such as compliance officers) who are not Administrators but wish notification when SSL Certificates are requested for a given organization.

HydrantCloud Managed PKI Service

Client and Device certificates may be used in a vast array of applications, each requiring a different technical configuration on the certificate itself, as well as different registration regimes. The HydrantID Enterprise Management Console is designed to simplify the complexity of choices, allowing organizations to rapidly fulfil their Public Key Infrastructure (PKI) needs.
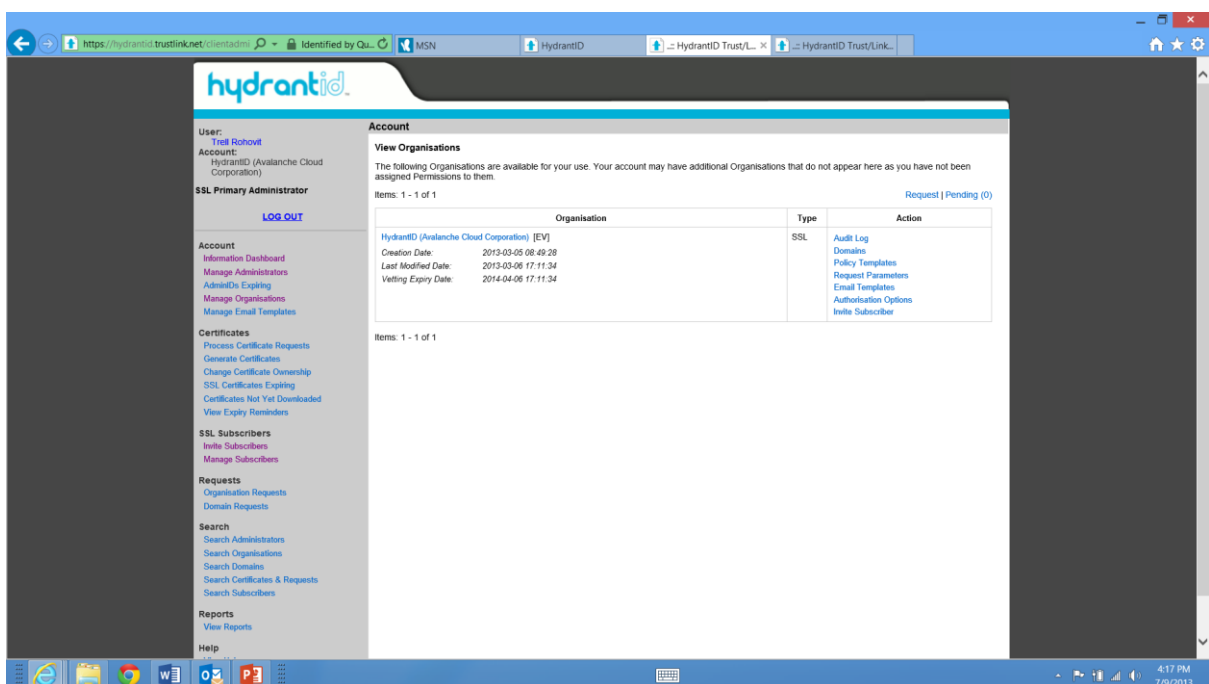
HydrantID Support works with your Administrators to select the appropriate certificate class from HydrantID's standard list and to configure it with the appropriate technical settings and issuance method.

The resulting templates make it simple for Administrators to invite new Subscribers with using pre-sets that integrate:

- *Fields:* The actual fields that will appear in the Certificates as well as their contents, which may be fixed or editable on a case-by-case basis.

- *Enrollment Options:* Depending on the Certificate class, invitations may be commenced by web form, Certificate signing request (CSR), or bulk upload. Workflow may include user confirmation of Certificate contents before issuance, and Certificates may be routed to a third party (such as a technical support desk) for installation.
- *Keying Options:* Flexible key generation options include client-side (including browser or token/smartcard) or Server-side (with optional private key archive).

To ensure appropriate security at the initial registration, the Administrator may either elect to use an existing shared secret, or to establish a "challenge and response" that the Subscriber will know how to answer. Once authenticated, the End User Subscriber may choose their own password for ongoing management of the Certificate (revocation and renewal).

Optional Web Services

The HydranrtID Enterprise Management Console operates as a standalone system for the request and fulfilment of Digital Certificate orders. However, for customers who may wish to integrate Certificate management into their own existing applications, HydrantID provides a web services API allowing them to programmatically:

- Request Certificates
- Inquire about a given Certificate's status
- Request Certificate revocation
- Create new Subscribers
- Download Certificates

Like the administrative areas of the system, access to the web service is controlled by Certificate-based authentication.   When a Certificate request is successfully received by The HydrantID Enterprise Management Console, the API will provide a unique ID which is to be stored and used in any future web method calls regarding that specific Certificate (such as requesting the Certificate's status or requesting to revoke the Certificate).

HydrantID Root Distribution

HydrantID Certificates are automatically trusted in a wide variety of browsers and operating systems.