Core iQ Server Configuration

Core iQ requires a dedicated Windows Server with no other applications or services that would interfere with its operation and automation. This server can be physical or virtual; however, virtual is always preferred due to ease of recovery. The server must be minimally configured

Minimum Specifications:

You need to roughly know your core data size in number of customers/members, and accounts. Having a general idea of these counts helps to properly size your server.

- OS: Microsoft Windows Server 2022.
- For clients requiring a previous version of Windows Server, Core iQ is currently backwards compatible with Windows Server 2019 and Windows Server 2016

Drive Space:

Onovative requests three partitions, sized according to the guidelines/calculations below be allocated to the Core iQ Server.

- A primary "**C**:" for the server OS, related software, and Core iQ Web Application
    - A minimum of 80GB+ of **free** hard drive space needs to be maintained on this drive for optimum performance.

- A secondary "**D**:" for housing the Core iQ database and Service applications
    - The data requirements for the drive housing the database can be calculated as a function of the number of customer/member and account records present on the client's core and ancillary platforms.
    - This can be roughly calculated at 150GB of storage for every 100,000 records. For example, a client with 100k customer/member records, 100k deposit records and 50k loan records would have a recommended drive allocation of: § 150GB + 150GB + 75GB = 375 GB Total disk space allocated to "D:"

- A tertiary "**E**:" for housing communication archival PDF files
    - The data requirements for the drive housing communication archival PDFs can be calculated as function of the anticipated communication volume on the Core iQ platform in conjunction with the FI's internal retention policy for the communication archival files.
    - The average archival PDF file is 1MB in size; however, a range of 500kb to 2mb is not unusual depending on the communication type (print versus email) and the complexity of the communication template created by the client.

- For a client sending an average of 50,000 communications per month with a 24 month retention policy the recommended drive allocation would be: § 50,000 * 1MB * 24 = 1.2TB Total Disk space allocated to “E:”
- Or, roughly 50GB of storage for each month of retention desired

PLEASE NOTE: Core iQ will chiefly perform read/write operations against the data and archival partitions. Please make sure that the drive you allocate is optimal for read/write operations. Slow read/write operations will have a huge impact on performance!

Memory/RAM:

Onovative strongly recommends a minimum of 32GB of available physical RAM be allocated on the Core iQ server. Additionally, RAM should be scaled out to support anticipated communication throughput requirements for the platform. For clients who need to realize the platform’s current maximum throughput, 64GB of physical RAM should be allocated to the Core iQ server.

CPU/Cores:

Onovative strongly recommends a minimum of (4) cores be allocated on the Core iQ Server. At this time a minimum of (8+) cores are required to leverage the platform’s current maximum throughput for communications.

Whitelisted Directories for Antivirus Software:

In addition to the below, you must ensure firewalls and any AV programs allow .zip files to be pulled and extracted onto the Core iQ server. Our live update packages arrive in .zip format from AWS S3. We have had several instances of network firewalls preventing the full retrieval and extraction of those .zip files updates, which can cause severe disruption to system operation.

The following directories should be whitelisted from Quarantine/Blocking and Scanning within any antivirus software installed on your server:

D:\Onovative
D:\Program Files\PostgreSQL
C:\inetpub\wwwroot
C:\Windows\Temp (Recommended, but not Required)
E:\Onovative\Onboarding

Server Role & Installed Features:

NOTE: Onovative will aid in any Role/Feature configuration provided that Minimum Specifications are met

- ***Common Http Features***
  - Static Content
  - Default Document
  - Directory Browsing
  - Http Errors
  - Http Redirection
- ***Application Development***
  - ASP.NET
  - NET Extensibility
  - ISAPI Extensions
  - ISAPI Filters
- ***Security***
  - Basic Authentication
  - Windows Authentication
  - Client Certificate Mapping Authentication
  - Request Filtering
  - IP & Domain Restrictions
- ***Management Tools***
  - IIS Management Console
  - IIS Management Scripts and Tools
- ***Microsoft .NET 4.7+***

Additional Configuration:

- Broadband Internet Access
- Firewall Rules Allowing Secured Requests To The Following:*
  https://ows.onovativeapp.com
  https://outcomeapi.onovativeapp.com
  https://webhooks.onovativeapp.com
  https://api.mainstreetinc.com/mail
  https://insights.onovativeapp.com
  https://api.cloudinary.com
  https://res.cloudinary.com
  https://s3.amazonaws.com
  https://api.onovativeapp.com

https://coreiq.onovativeapp.com
https://hasura.coreiq.onovativeapp.com/
Note: Web browser needs to be able to make a web socket connection to this URL.

- No Proxy Server running.

- Internal DNS CNAME Entry to Point "coreiq" to the VM, *IF… You do not require an SSL Certificate for Internal Traffic*

    - A CNAME entry is so people on your LAN can access Core iQ easily at http://coreiq
    - However, if you want SSL encryption of your "internal" network traffic to the server, please let us know whether you wish to use and install a self-signed certificate or a purchased one. If you use a certificate, users will access Core iQ at the fully qualified name, i.e. https://coreiq.yourdomain.local.**

- External DNS Zone File Entries for Email White-labeling***

    - These entries should be provided by Onovative, and will be validated by Onovative once records have had a chance to propagate
    - These are CNAME, DKIM entries that inform the rest of the world that email is being sent legitimately on your behalf. This follows best practices.
    - Onovative will obtain a dedicated IP address for any emails being sent on your behalf to mitigate any risk of blacklisting
    - See DMARC below for more information.

*Where customers and their sensitive financial data is housed in the data warehouse on your own secured server, less sensitive data is transacted over secured channels with encrypted keys for the fulfillment of certain services and communications provided by Core iQ. Requests to these APIs only originate from the trusted side of your firewall. You do NOT need to open a port to allow traffic "from" the outside world. You will not see requests from these external sites; only a response to a request made from the trusted side of the firewall.

- https://ows.onovativeapp.com
  Manages global contact preferences to record and honor customer opt-outs from emails and SMS Text messages. Provides statistics on Core iQ health and usage.

- https://outcomeapi.onovativeapp.com
  For retrieval of email statistics and survey results.
- https://webhooks.onovativeapp.com
  Helper for retrieval of email statistics and survey results.
- https://api.mainstreetinc.com/mail
  Provides printing of letters and postcards. No customer data lists are uploaded for fulfillment. Finalized artwork is rendered per request for printing and postage to a specific customer.
- https://api.cloudinary.com
  Content Delivery Network for images included within emails
- https://res.cloudinary.com/
  Content Delivery Network for images included within emails
- https://s3.amazonaws.com
  For retrieval of Live Updates posted for Core iQ secure consumption. For creation of survey templates accessed by intended survey recipients.
- https://api.onovativeapp.com
  For retrieval of cloud-based metrics to locally hosted dashboards in the Core iQ platform. These metrics include email events and survey responses.
- https://prod.onovativeapp.com
  This endpoint is required for delivery of certain cloud provided application interfaces that can change frequently.
- https://coreiq.onovativeapp.com/
  This endpoint is leveraged by Core iQ for performing batch based interactions with cloud based data and resources.
- https://hasura.coreiq.onovativeapp.com/
  This endpoint is leveraged by Core iQ for performing batch based interactions with cloud based data and resources.
- https://pinpoint.us-east-1.amazonaws.com
  Provides anonymous metrics on user activity and experience within the Core iQ application. Onovative support and product development staff rely on these metrics to ensure proper behavior and improve user experience within the.
- https://cognito-idp.us-east-1.amazonaws.com
  Provides management of client user and user groups for anonymous metrics and authentication to cloud based resources.
- https://cognito-identity.us-east-1.amazonaws.com
  Provides management of client user and user groups for anonymous metrics and authentication to cloud based resources

**We do recommend encrypting Core iQ network traffic. This is usually accomplished with an SSL certificate, applied to the intranet site hosted in IIS on the server you've provisioned. There are two basic ways to obtain assign an SSL certificate to the Core iQ host. Each has its own pros and cons.

1) Purchasing a certificate from a global "Certificate Authority":

- This is no different than acquiring a certificate that you assign to your website. GoDaddy is an example provider for SSL certificates, but there are others that are considered as a "Certificate Authority" (CA) issuer.
- The up-side is that most client machines are already provisioned to "trust" the certificate issued by a CA. The certificate is automatically downloaded to the trusted root without any required action on the part of the client.
- The down-side is cost. These certificates are not free and must be renewed before they expire.
- In this scenario, you will likely need to obtain a Certificate Signing Request (CSR) on the Core iQ server itself from within IIS. Onovative can provide guidance in this regard, if you require.
- Once you obtain the certificate from the CA, yourself, or Onovative should you wish, can apply it to Core iQ and we will turn off access over the standard Port 80. This will force use of the certificate on Port 443, encrypting data in transit between the server and the client browser on your network.

NOTE: If you have purchased a "wildcard" certificate, you may be able to use it on the Core iQ server depending on the naming convention used to resolve to the server.

2) Create a "Self-Signed" certificate on the server itself:

- This type of certificate is equally valid and will encrypt traffic on your network. There is no cost. Once created, it is the client's responsibility ensure your client browsers actually use the certificate.
- The down-side with this type of certificate is that you commonly have to distribute these to client machines. They are not automatically trusted.
- Usually, a group policy can be created that causes the certificate to be downloaded to the client. If this is not possible, the certificate will need to be manually installed to the trusted root certificate store on "each" client machine.

Which should you choose? That is up to you and your policies. We have applied more self-signed certificates than those issued by a CA, but it usually comes down to tolerance for added cost. **Regardless, once the SSL cert is applied and enforced, you must be sure to update/push a new group policy (GPO) to add the app URL to the list of trusted local intranet sites in order to accommodate user access.**

DMARC Email Authentication

*****Announcing New DMARC Policy – What the new DMARC requirements mean for Core iQ users**

As a strategic email partner for financial institutions, it is crucial to keep Core iQ customers ahead of the curve on the latest email security standards to ensure your email deliverability and sender reputation are safeguarded against digital threats. Recently, industry giants like Google and Yahoo announced significant changes to their email requirements that will be enforced beginning in February 2024.

What are the new DMARC requirements by Google and Yahoo?

Beginning February 1, 2024, email providers Google and Yahoo will begin enforcing Domain-based Message Authentication Reporting and Conformance (DMARC) authentication for email sends from bulk senders (i.e. those that might send 5,000+ emails per day). DMARC is a standard that builds on Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) email authentication methods. DMARC communicates a policy to mailbox providers letting them know what they should do when they receive an email that fails an SPF, DKIM, or SPF and DKIM check purporting to be from your domain (possibly spoofed).

Why does this impact Onovative's Core iQ users?

To date, Onovative has ensured high deliverability rates by leveraging automated security from our email API, SendGrid, for both SPF and DKIM, requiring our clients to have the proper DNS entries published on their side and validated on our side, as described above.

However, DMARC is a higher level of authentication which you may or may currently have in place. In anticipation of this change, the email API Core iQ utilizes, SendGrid, made a change to their authentication configuration by adding a DMARC protocol with baseline restrictions in order to satisfy the new ESP requirements.

Because of this change, we are alerting Core iQ users so that you continue to have high volume deliverability to Google and Yahoo email service providers.

What do Core iQ users need to do?

Set up DMARC email authentication for your sending domain. If your financial institution does not yet have a DMARC policy in place, you will need to create one and add the requisite and supplied entries for validation**.** If you aren't sure if you already have DMARC in place, you can check for free through Valimail.

Below are some resources to help your financial institution implement DMARC effectively. Once these changes have been implemented, please reach out to your Onovative Implementation project coordinator to authenticate on our end.

https://sendgrid.com/en-us/blog/gmail-yahoo-sender-requirements

We're Here To Help

We understand these new requirements can be confusing and we're here to assist you however we can. If you have questions or concerns about these changes and how they will impact your email communications, please don't hesitate to contact our team.

Additional Resources & Information on DMARC

If you have DMARC authentication in place for outbound email or are needing to add it, the following info has *usually* been adequate to successfully accommodate Core iQ's email service. The DNS Zone File Entries sent to you for publishing/white-labeling include both the SPF record and DKIM entries you will need in this regard. With respect to SPF, the correct entry would be either "sendgrid.net" and/or your dedicated IP address contained in the file.

Below are a few relevant articles SendGrid (Core iQ Email API) make available on the topic. Let us know if you have any questions.

https://docs.sendgrid.com/ui/sending-email/dmarc
https://sendgrid.com/en-us/blog/what-is-dmarc
https://docs.sendgrid.com/ui/sending-email/how-to-implement-dmarc
https://dmarc.org/wiki/FAQ#My_organization_uses_third-parties_senders.2C_how_can_I_get_them_DMARC_compliant.3F
https://support.sendgrid.com/hc/en-us/articles/360041356934-Troubleshooting-Email-Delivery-Failures-due-to-DMARC
https://sendgrid.com/docs/ui/account-and-settings/troubleshooting-sender-authentication/#manually-validating-records