Cherwell Software Hosted Environment

Cherwell Software, LLC ("Cherwell") provides an efficient, expedient, and secure hosted environment so that customers are guaranteed exceptional performance and reliability.

This document looks at the key areas of Cherwell's hosted environment:

- Architecture.
- Data availability.
- High Availability.
- Security.
- Disaster recovery.
- Reporting.
- Integration with third party applications.

CreekPointe
CHERWELL PARTNER™

www.creekpointe.com | info@creekpointe.com
864.297.4959 | +1 800.613.1426

Cherwell SOFTWARE™

www.cherwell.com | info@cherwell.com
+1 719.386.7000 (US) | +44 (0) 1793 544888 (EMEA)

Hosting Architecture

Cherwell Service Management® ("CSM") clients connect with the Cherwell datacenter over the internet via Hypertext Transfer Protocol Secure (HTTPS), a secure communications protocol. Users can access the datacenter using an auto-deployed client on their machines, a web browser[1], or a mobile device.

For integrations with services or third party applications, a site-to-site Virtual Private Network (VPN) connection is made, which is restricted to the customer's individual server(s).

Figure 1 shows an overview of Cherwell's hosting architecture.

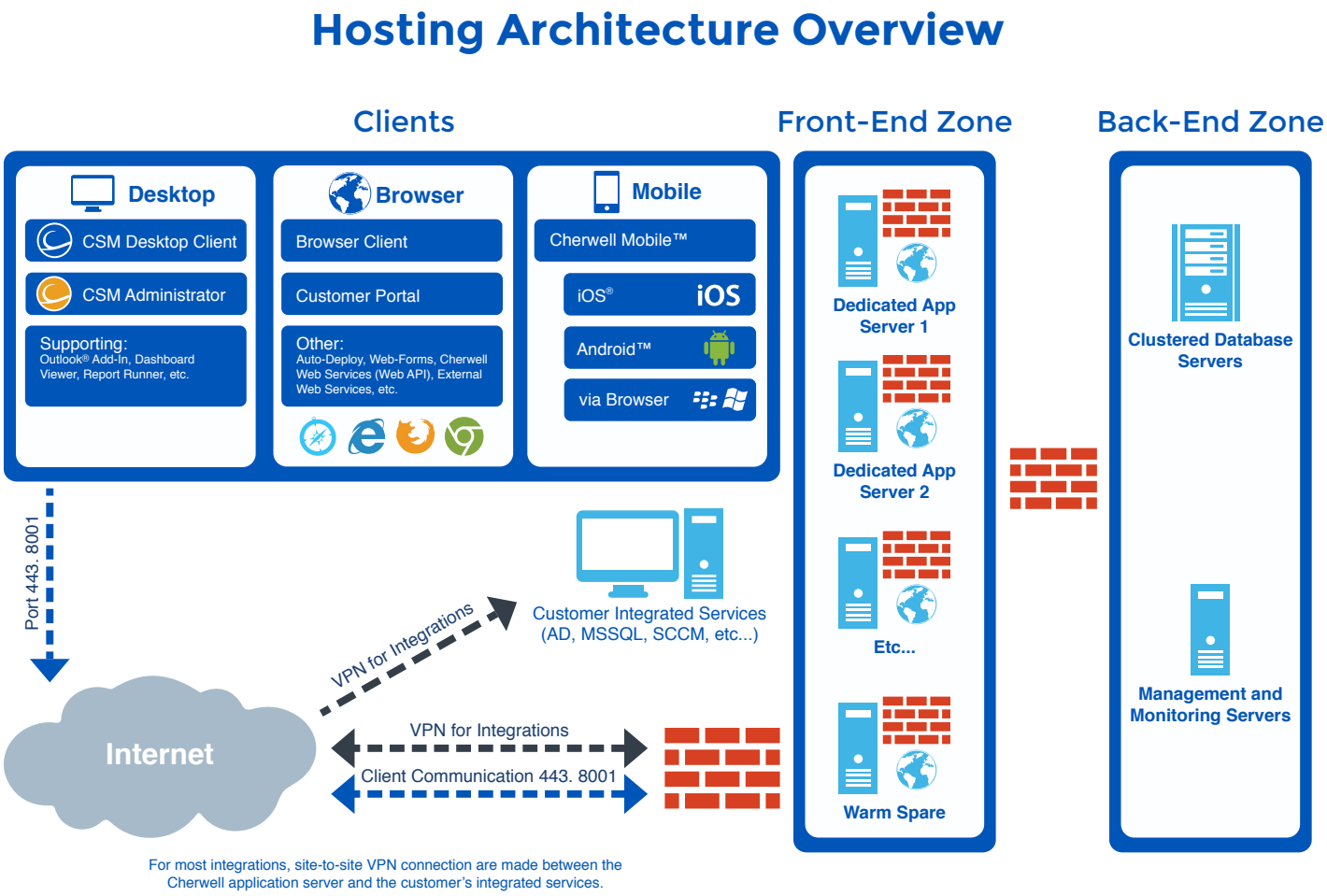

Figure 1. Hosted Architecture Overview

The connection to the datacenter is protected by:

- Firewalls.
- Intrusion Detection Systems (IDS).
- Intrusion Prevention Systems (IPS).
- Anti-virus.
- Anti-malware.

Data in motion is encrypted as it travels to and from the customer's location and the datacenter.

[1]No browser plug-ins required, refer to latest system requirements and specifications for supported browsers.

Hosting Offering

Cherwell offers the following for hosted customers:

- Up to two (2) hosted instances (additional hosted instances at extra cost).
- Data backups (for purposes of disaster recovery).
- 24x7 emergency support.
- Secure Socket Layer (SSL) encryption.
- Up to three (3) hosted e-mail accounts. E-mail accounts are used to provide communication services and are not intended to be used for bulk e-mail storage.
- Site-to-site VPN tunnel (priced separately).
- Cherwell Discovery and Inventory™ (priced separately). Note: This requires the installation of a service in your local environment.

Please contact your Cherwell representative for pricing information.

Monitoring

In addition to our datacenter providers' monitoring platforms, Cherwell uses several monitoring platforms to ensure that services are always available 24x7. Monitoring includes:

- CPU utilization.
- Memory usage.
- Disk IO.
- Disk space.
- Network performance.
- Cherwell application services.
- Database connectivity.
- Intrusion and security related events.
- Backup jobs.

Performance monitoring reports are available upon request.

Customer Server and Data Isolation

At the datacenter, application servers present CSM to each customer. Host-based firewalls isolate communications between application servers. Each server has host-based IDS, IPS, and anti-virus/anti-malware agents.

Data Availability

Cherwell offers an uptime of 99.98% availability per month, except for excused outages.

Cherwell datacenters are designed to give customers the highest availability possible using the following technologies and methods:

- Front-end/application servers that can easily be replaced as needed, leveraging the latest virtualization technologies.
- Redundant data connections to multiple carriers to help ensure that internet connectivity will not be lost.
- Physical Environment redundancy across all levels, with n+1 power and environmental systems.

Excused Outages are defined as unavailability of the Licensed Software caused by:

- Scheduled maintenance.
- Customer's systems or customer's actions/inactions.
- Circumstances beyond Cherwell's control, or the control of Cherwell's authorized agent or service provider, including without limitation, acts of God, acts of Government, flood, fire, earthquakes, civil unrest, acts of terror, strikes or other labor problems, equipment and telecommunications failures, delays, attacks or intrusions, provided Cherwell Software or its authorized agent or service provider takes reasonable and commercial care to prevent such failures, delays, attacks or intrusions.

High Availability

Within the U.S., Cherwell provides High Availability with two (2) hot sites, Denver, CO and Ashburn, VA, and one (1) warm site, Colorado Springs, CO. Customer data is replicated between the two (2) hot sites in real time using Microsoft SQL AlwaysOn technology. Traffic can be switched between the three (3) sites using traffic load balancers, which route DNS requests to the appropriate datacenter.

Clustered VMware™ ESXi™ servers with Distributed Resource Scheduler (DRS) allow resource optimization under changing conditions. Multiple database clusters are deployed to allow real time failover protection to minimize downtime and provide redundancy. Database traffic types are separated into appropriate clusters and optimized for performance. Guest servers are constantly monitored for performance within the hosted environment.

If a customer requires a VPN, two (2) VPN tunnels will be required for High Availability failover between hot datacenters.

Figure 2 shows Cherwell's High Availability architecture overview.

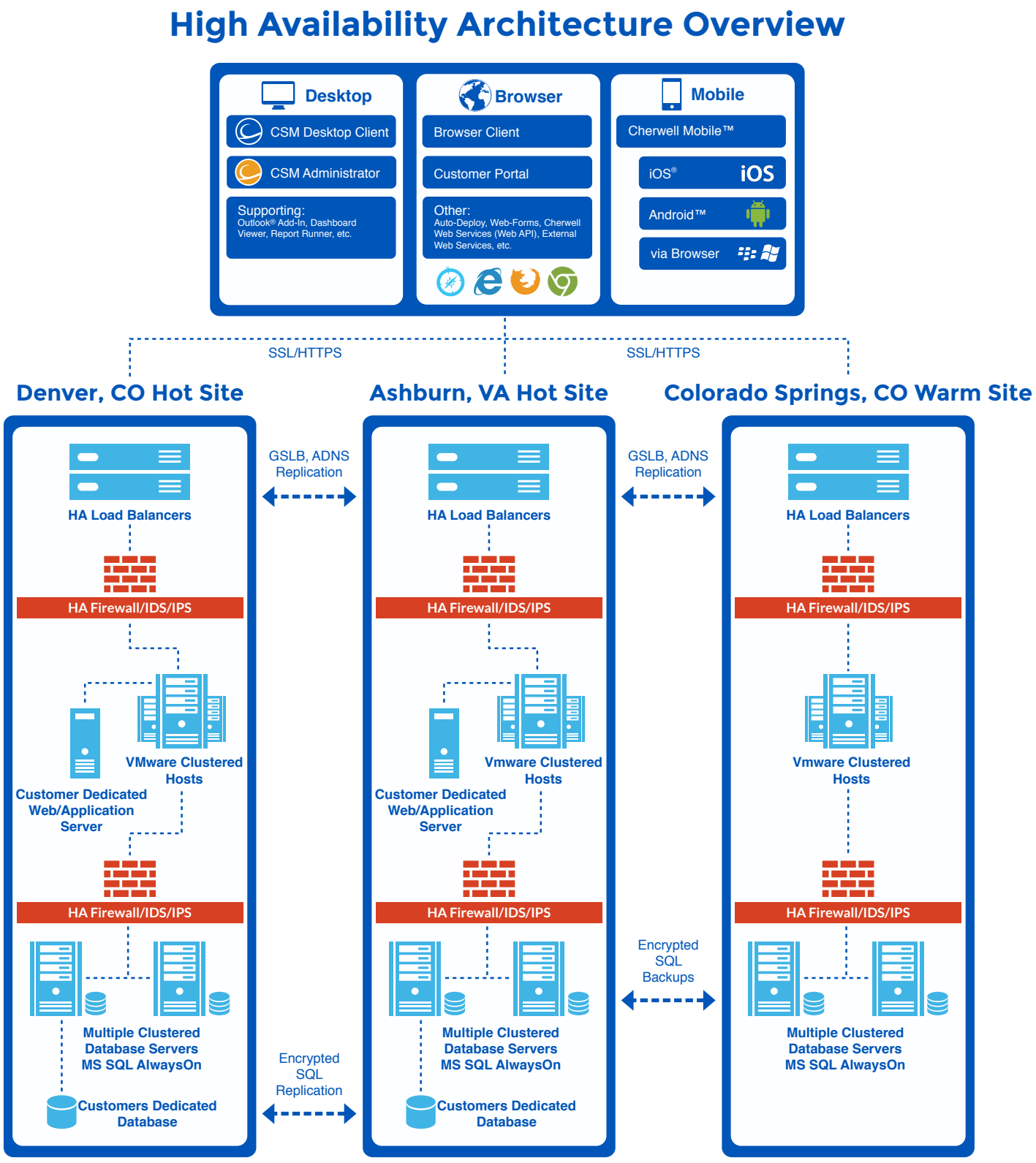

Figure 2. High Availability Architecture Overview

Security

Security is a top priority for Cherwell to support its customer's data residing in Cherwell's hosted environment.

Physical

Physical security is managed by the datacenter providers and is regulated and controlled via their SAS 70 Type II/ SSAE16 practices and standards. These practices and standards include, but are not limited to:

- Established and regularly reviewed security policies.
- Controlled entry, mantraps, biometrics, full camera coverage, and bullet proof glass around the Network Operations Center (NOC).
- 24x7 monitoring and security.

Network

Cherwell uses two (2) models of datacenter providers:

- **Managed services:** Our managed services providers manage all security controls for:
  - Telecommunication infrastructure.
  - Network infrastructure.
  - Routing.
  - Switching.
  - Firewalls.
- **Co-location:** In our co-location datacenters, Cherwell manages these security controls. Cherwell has established a set of security configurations that have been applied to all environments for devices within Cherwell's control, including:
  - Network segregation.
  - Firewall configurations.
  - Site-to-site VPN configurations.
  - Access control lists.

Back-end Servers

Server security is managed by our Cherwell Datacenter Administrators.

Cherwell uses a secure configuration that complies with the Center for Internet Security (CIS) benchmark standards. All computers are domain joined and security policies are enforced via group policy and scripts. Accounts, access, authorization, and authentication are tightly controlled and monitored. Customer application servers are isolated, via host-based firewalls, from each other. The back-end services, such as domain, management, and databases are segregated from all application servers.

The concept of *least privilege* is in practice and enforced through administrative policy.

Application

Direct access to the server application in the hosted environment is allowed only by authorized Cherwell Datacenter Administrators.

The only method a customer can use to access their application is through a 3-tier connection over the internet, either via the CSM Desktop Client, the CSM Administrator tool, or the server's website.

Client connectivity using any of these methods is encrypted and digitally signed to and from the application server using HTTPS over SSL.

Security Testing

Cherwell performs a series of security audits and assessments to ensure that an adequate level of security is maintained. These tests include the following:

Security Test	Performed By	Frequency
Physical Site Visit	Cherwell Software	Annually
SaaS Enterprise Information Security Assessment	Third Party	Annually
Internal Vulnerability Assessment	Cherwell Software	Monthly
Internal Process and Procedure Audit	Cherwell Software	Annually
SAS 70 Type II/SSAE16 Audits	Datacenter Providers	Annually

Restrictions

The Cherwell hosting model must be managed and maintained in a secure manner. Because this service is available over the internet, Cherwell must have configuration standards and security restrictions that customers might not typically have on servers in their own internal environment.

Below are some of the restrictions imposed when CSM is deployed in Cherwell's hosting environment:

- Only authorized Cherwell employees will have direct login access to the operating system of the customer's application server. These Cherwell employees include:
  - Support.
  - Professional Services.
  - Datacenter Administrators.

Cherwell will only directly view customer data on a case by case basis, for support purposes, and only after obtaining permission from the customer.

- Only the Datacenter Administrators have direct access to the database server. No other Cherwell employee, partner, or customer may have direct access to these servers, or create systems that access these servers directly.
- The only approved service that can access the database server directly is the Cherwell service running on the customer's application server.
- Direct database customizations that are not completed within CSM are rarely done and only in the context of using SQL views to enhance functionality. CSM has a feature that supports this within the CSM Administrator tool and applying a SQL view is only approved on a case by case basis after a proper review by the Cherwell Datacenter Administrators. Customers should work with a Cherwell Professional Services Consultant or Support representative to determine the need for this type of customization.
- Cherwell redirects all internet Browser Applications and portal pages to HTTPS and manages the SSL certificates. Custom hostnames are provided [(*customer/company*)].cherwellondemand.com].
- In addition to the provided domain URL, customers can also use their own domain name and Cherwell will purchase a SANS SSL certificate to support multiple subject names. If a customer selects this option, the customer's web domain administrators will need to approve Cherwell's use of using the domain for browser app access on the SSL certificate.
- The installation of third party applications and/or services are not allowed on the hosted environment servers.

Access to Data

Datacenter Employees

Cherwell datacenter providers' employees do not have direct access to Cherwell servers or customer data. They maintain the physical hardware and managed services only, and are under strict contractual agreement not to access Cherwell Software customer data.

Cherwell Software Employees

Access to customer data is restricted to only authorized Cherwell employees. Cherwell employees accessing the datacenters undergo background checks, are governed by non-disclosure agreements and are required to have security awareness training.

Customer Access

Customers will not have direct access to the hosted Cherwell server or to the database server that hosts their data. Backups of the data can be obtained at any time using the CSM Administrator tool, and the customer is responsible for this function.

Disaster Recovery Plan

High Level Plan

A disaster is defined as any event that would cause Cherwell to breach the recovery time objectives. If an event is verified, Cherwell will begin the process of bringing up customer servers and data in the backup datacenter. DNS records are changed to point to the new service location. After the new services have been verified, customers are notified that their services have been restored. After the outage has been resolved, customers are moved back to their datacenter of origin. This process is designed for minimal impact to the customer, and communication to the customer takes place throughout the process.

Backups

All backups are encrypted both at rest and in transit. Backups are made directly to disk and replicated to a secondary geographically disperse location. Differential hourly backups are performed and stored for five days. Then, daily backups are stored for thirty-one (31) days. Customers are encouraged to make their own backups of the application data using built-in functionality using the CSM Administrator tool.

Recovery Point Objective (RPO)

The RPO for data recovery is to the last hourly backup.

Recovery Time Objective (RTO)

The RTO is two hours or fewer for production instances. Production will be restored first. The RTO for any test or development instance is on a case by case basis.

Business Continuity Plan

The main goal of the business continuity plan is to provide a high level overview to ensure ongoing service to customers in the event of a disaster.

Geographic Location

Colorado has been the state of choice for numerous Fortune 500® companies, such as FedEx®, Walmart®, and Progressive Insurance®. Having two geographically dispersed datacenters with multiple telecommunication carriers provides ongoing service to customers in the event of a disaster.

Cherwell Employees

All employees that are involved in customer care and datacenter monitoring are equipped with company issued cell phones and laptops configured with secure VPN capabilities. Additionally, employees have access to either a mobile Wi-Fi connection or cell phones equipped with tethering capabilities. An on-call rotation is in place to ensure 24x7 coverage for Cherwell's hosted services. An escalation call tree is in place in the unlikely event the primary technical resource is unable to respond to an event.

Applications

Mission critical applications are designed and maintained in a manner that does not rely on any physical office infrastructure.

Development applications, including source code, are hosted in geographically disparate environments, ensuring that our developers can continue to support the application without physical access to the office.

Network Access

Access to mission critical applications is not 100% reliant on Cherwell's internal network infrastructure. Key employees can access applications via public internet and secure VPN connections.

Phone Access

In the case of a disaster, Cherwell's main support number can be routed to key employees' company issued cell phones ensuring uninterrupted service to Cherwell customers.

Reporting

Ad-Hoc Reporting

Performance status reports are available upon request. These reports include the following metrics:

- Performance
  - Average processor
  - Average memory
  - Average network
  - Database size
  - Uptime Statistics

Outage Reporting

- Notifications will be sent upon discovery of a service outage via e-mail.
- Notifications will include a recovery time estimate.
- Upon resolution of the outage, an additional notification will be sent advising the customer that the services have been restored.
- A post-outage incident review will be conducted, and the findings, including any remediation steps, will be sent to the customer via e-mail.

Maintenance Reporting

- Maintenance is performed on a monthly basis.
- Maintenance windows are established by Cherwell and communicated to the customer at the start of the new calendar year.
- A notification of upcoming maintenance will be sent out one week ahead of the scheduled time and on the day of the maintenance via e-mail.
- When maintenance has been completed, a notification will be sent via e-mail.

Datacenter Facilities Reporting

Australia	Canada	United Kingdom	United States of America
Brisbane, NSW	Kelowna, BC	London	Denver, CO
	Barrie, ON	Manchester	Ashburn, VA

Cherwell's datacenters are SAS 70 Type II or SSAE16 compliant. Details and audit reports for each datacenter are available upon request and include:

- **Physical security** is maintained through a multi-layer security approach with biometrics, card access, 24x7 security guards, monitoring of mission critical systems, as well as surveillance and access control.
- **Datacenter power** is achieved through multiple, redundant power distribution units, emergency generators, and UPS systems.
- **NOC** is on-site for proactive maintenance and repairs, providing 24x7 remote hands, and mechanical and electrical monitoring, including branch-circuit monitoring by certified technicians.
- **Datacenter connectivity** is ensured with redundant telecommunication connections to multiple carriers.
- **Environmental controls** include an N+1 cooling system, dual-interlock, dry-pipe pre-action fire suppression system, as well as 20-ton Computer Room Air Conditioning (CRAC) units to provide cooling.

Integration with Third Party Applications

Site-to-Site VPN

A site-to-site VPN is used only for the purpose of integrating with other third party applications and systems. It is not necessary for most e-mail configurations and Active Directory® imports, but would be required for all other integrations, including Active Directory integrated authentication.

Customers are responsible for providing and maintaining a VPN device capable of establishing an industry standard IPsec tunnel.

Cherwell will provide the configuration information necessary for establishing the tunnel and will help troubleshoot connections; however, the configuration of customer's device is the sole responsibility of the customer.

There are several Microsoft® SQL Server® and OLEDB data integrations with other applications that can be accomplished within the hosting environment. The most commonly requested integrations include:

1. **LDAP:** CSM integrates with Active Directory database or an Lightweight Directory Access Protocol (LDAP)-compatible provider for the purpose of integrated authentication or pulling of directory information. For directory information data pulls, CSM will typically install a small local scheduling service into the customer environment that will then replicate that data securely to the hosted environment. Integration can also be accomplished across a site-to-site secure VPN tunnel.

2. **E-mail:** CSM has the ability to send e-mail, as well as monitor e-mail inboxes for incoming requests. To monitor an inbox, the customer's e-mail services must be accessible from outside their network. Please see the chart below for supported protocols. If customers do not want to use their own e-mail services, Cherwell can supply up to three e-mail addresses at no additional charge.

Protocol	Microsoft® Exchange 2003 and Below	Microsoft® Exchange 2007 and Above	Non-Exchange
POP3	✓	✓	✓
IMAP	✓	✓	✓
SMTP	✓	✓	✓
WebDAV		✓	

3. **Other Services:** CSM is highly configurable, and custom integrations are often used in the hosting environment. These custom integrations have included configuration management platforms, databases, phone systems, and password reset tools.

Do you need a site-to-site VPN tunnel for CSM integrations?

Integrations can be accomplished in multiple ways:

- For some types of integrations, such as Active Directory data pulls, CSM can install a local service.
- CSM also has a service for password reset integrations.
- CSM can integrate with Microsoft® Outlook® Web App over the internet without any special configuration.
- Integrations, such as Microsoft® System Center Configuration Manager (SCCM), Active Directory authentication, and anything behind your corporate firewall, require a site-to-site VPN tunnel.
- CSM also integrates with Security Assertion Markup Language (SAML) 2.0 providers for authentication over the web, which does not require any additionally installed service(s) or a site-to-site VPN tunnel.

As a general rule, if a customer wants a service that is secured behind the customer's corporate firewall to be integrated with CSM, the customer will need a site-to-site VPN tunnel.

Working with a Cherwell Professional Services Consultant is the best way to understand each organization's specific integration needs.

Conclusion

This document describes Cherwell's hosting environment, including architecture, data availability, High Availability, security, disaster recovery, reporting, and integrations with third party applications. The information contained in this document is subject to change.

As Cherwell continues to grow and add more customers, its best practices, approach, and hosting capabilities will continue to evolve and improve. This document will be updated as needed to reflect these changes.