Siebel CRM

Siebel Security Hardening Guide

Siebel Innovation Pack 2016

E24815-01

April 2016

Siebel Security Hardening Guide, Siebel Innovation Pack 2016

E24815-01

Contents

4 Securing the Operating System

5 Securing the Siebel Database

6 Securing Siebel Business Applications

7 Implementing Auditing

8 Performing Security Testing

A Supported Security Standards

B Default Port Allocations

Index

List of Figures

List of Tables

Preface

This guide covers Siebel Security Hardening implementation and administration.

Audience

This guide is intended for system administrators, database administrators, developers, security groups, and IT staff involved in securing environments for Siebel Business Applications.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at

`http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Related Documents

For more information, see the following documents on Oracle Technology Network:

- *Siebel Security Guide*
- *Siebel System Administration Guide*
- *Siebel Applications Administration Guide*
- *Siebel Remote and Replication Manager Administration Guide*
- *Siebel Installation Guide* for the operating system you are using

Conventions

The following text conventions are used in this document:

Convention	**Meaning**
italic	Italic type indicates book titles, emphasis, a defined term, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, code in examples, text that appears on the screen, or text that you enter.

1

What's New in This Release

This chapter describes new product features.

What's New in Siebel Security Hardening Guide, Siebel Innovation Pack 2016

No new features have been added to this guide for this release. This guide has been updated to reflect only product name changes.

Note: Siebel Innovation Pack 2016 is a continuation of the Siebel 8.1/8.2 release.

What's New in Siebel Security Hardening Guide, Siebel Innovation Pack 2015

Table 1–1 lists the changes described in this version of the documentation to support this release of the software.

Note: Siebel Innovation Pack 2015 is a continuation of the Siebel 8.1/8.2 release.

Table 1–1 New Product Features in Siebel Security Hardening Guide, Siebel Innovation Pack 2015

Topic	Description
"About Using Transport Layer Security with Siebel CRM" on page 2-4	New topic. Secure Sockets Layer (SSL) v3.0 communications encryption is not supported for environments with security requirements. It is recommended that you use the Transport Layer Security (TLS) protocol instead of SSL.
"Encrypting the jndi.properties File" on page 3-19	New topic. Describes how to encrypt the jndi.properties file so that the user credentials in the file will not appear in clear text format.

2

Overview of Security Threats, Recommendations, and Standards

This chapter provides introductory information about securing Oracle's Siebel Business Applications and the infrastructure and environment in which they operate. This chapter includes the following topics:

About This Guide

This guide provides recommendations for safeguarding your Siebel CRM deployment from internal (intranet) and external (Internet) security threats. The most important reason for securing an application is to protect the confidentiality, integrity, and availability of an organization's critical information. However, to protect your Siebel Business Applications data, you must secure both your Siebel Business Applications and the computing environment in which they run.

Siebel Security Hardening Guide (this book) and *Siebel Security Guide* provide the information you need to protect your Siebel Business Applications deployment:

- *Siebel Security Guide* describes the Siebel security architecture and security concepts. It outlines the security controls provided by Siebel Business Applications, and gives detailed procedural information on how to implement these controls to secure your application.
- This guide, *Siebel Security Hardening Guide*, describes how to harden your Siebel Business Applications deployment.

  Hardening is the process of protecting your computer network and applications from internal and external security threats by minimizing the areas of security vulnerability. Examples of hardening tasks include removing unnecessary software, services and utilities, disabling unused user accounts or login IDs, and setting up intrusion-detection systems. This guide provides detailed procedural information on implementing Siebel security controls only where such information is not provided elsewhere on the *Siebel Bookshelf*.

Note: The *Siebel Bookshelf* is available on Oracle Technology Network (http://www.oracle.com/technetwork/indexes/documentation/index.html) and Oracle Software Delivery Cloud. It might also be installed locally on your intranet, or on a network location.

This guide applies to Siebel CRM version 8.1 and 8.2 and is intended for Siebel administrators, security groups, and IT staff involved in securing environments for Siebel Business Applications. It is assumed that users are familiar with Siebel Business Applications, their architecture, and with the general security principles within an IT environment.

Note: This guide contains recommendations for securing the infrastructure in which Siebel Business Applications operate. You are responsible for ensuring all the security procedures recommended by your operating system and database vendors have been completed to provide a secure environment for Siebel Business Applications.

Security Threats and Vulnerabilities

To secure your Siebel Business Applications environment, you must understand the security threats that exist and the typical approaches used by attackers. This understanding helps you to identify the correct countermeasures that you must adopt. The common security threats include:

- Computer viruses (malware)
- Code injection
- SQL injection
- Cross-site scripting (XSS)
- Denial of service attacks (DoS)

The following practices can make your applications vulnerable to malicious attacks:

- Using weak passwords
- Moving data between applications, computers, and sites
- Allowing information leaks
- Allowing nonsecure coding practices when configuring Siebel Business Applications

Monitor security sites for information on newly discovered vulnerabilities affecting third-party components or applications that are integrated with Siebel Business Applications software. Some of the well-known Web sites that contain information on security incidents with vulnerabilities and patches are as follows:

- www.cert.org
- www.sans.org
- www.insecure.org
- www.cisecurity.org
- www.securityfocus.com (hosts the Bugtraq mailing list)

Perform security risk assessments regularly to identify possible security vulnerabilities in your environment, then address any issues. For information on this task, see Chapter 8, "Performing Security Testing." For general information on preventing security attacks and vulnerabilities in your environment, see "General Security Recommendations" on page 2-3.

General Security Recommendations

Align the policies you create to secure your Siebel Business Applications environment with the overall security policies and principles adopted by your organization. Some of the general policies recommended to help protect your Siebel Business Applications deployment and infrastructure include the following:

- Restricting network access
- Following the principle of least privilege when setting up access controls
- Monitoring activity by enabling a minimum level of logging (auditing and reviewing)
- Keeping up-to-date with the latest security information
- Configuring accounts securely, including securing session management
- Setting security parameters
- Running security-maintenance reports regularly
- Enforcing secure coding practices, for example, data validation, when creating custom code and scripts
- Encrypting Web and network communications and sensitive data in the Siebel database, for example, credit card numbers and passwords
- Installing approved enterprise-wide antivirus software to protect servers and workstations, and updating virus pattern files on a periodic and emergency basis as recommended by the vendor

Patch Management

Implement a patch management process to make sure that all the software in your environment is updated with the latest software versions and security patches. You must make sure all updates and patches for Siebel Business Applications are applied. Also make sure that all updates are applied for the other software that is required to run Siebel Business Applications, but that is not shipped by Oracle. Some examples include your operating system software and browser software.

Critical Patch Updates for Siebel Business Applications

Oracle uses critical patch updates to release security patches for all its applications, including Siebel Business Applications. Critical patch updates are issued each quarter and consist of multiple security fixes in one patch.

For a list of the latest critical patch updates and security alerts for Siebel Business Applications available from Oracle, and for information on security vulnerabilities fixed in a critical patch update, go to the Oracle Critical Patch Updates and Security Alerts Web site at

`http://www.oracle.com/technetwork/topics/security/alerts-086861.html`

Oracle provides information about product security vulnerabilities only as part of the critical patch update or Security Alert notification process.

Security Standards and Programs

Siebel Business Applications adhere to a range of common industry standards relating to security so that customers can choose a security infrastructure that best suits their specific business needs. For a list of the technical standards supported with Siebel Business Applications, see *Siebel Security Guide*.

Siebel Business Applications also support the following standards:

- Payment Card Industry Data Security Standard (PCI DSS)
- Common Criteria for Information Technology Security Evaluation (Common Criteria) standard
- Federal Information Processing Standard (FIPS) 140

For information about Siebel Business Applications support for the PCI DSS, Common Criteria, and FIPS standards, see Appendix A, "Supported Security Standards."

> **Note:** Siebel Business Applications do not provide a client that supports the Security Assertion Markup Language (SAML) standard.

About the Oracle Software Security Assurance Program

Siebel Business Applications are developed and maintained in accordance with the Oracle Software Security Assurance program, which incorporates security best practices in the following areas:

- Secure development process
- Critical patch updates
- External security validations
- Security information and best practices

For further information on the Oracle Software Security Assurance program, go to

`http://www.oracle.com/us/support/assurance/index.html`

About Using Transport Layer Security with Siebel CRM

It is strongly recommended that you implement Transport Layer Security (TLS) encryption for all of the following services and communication paths in a Siebel CRM implementation:

> **Note:** The use of Secure Sockets Layer (SSL) v3.0 encryption for environments with security requirements is not supported by Oracle for Siebel CRM as a result of security vulnerabilities discovered in the design of SSL v3.0.

- For communications between Siebel Web server and Siebel Web Client.
- For communications between Siebel Server and the Web server.

- For encryption of SISNAPI communications between Siebel Enterprise components, for example, communications between the Siebel Server to Siebel Web server (SWSE), or between Siebel Servers.
- For communications between an LDAP or ADSI security adapter and a directory server.
- For communications using the Siebel Business Applications external interfaces (EAI), which use Web services to send and receive messages over HTTP.
- For communications between Siebel Server and an email server, including encryption for SMTP, IMAP, and POP3 sessions between Siebel Server and an email server.

For more information, see Chapter 3, "Securing the Network and Infrastructure" which includes information about the following:

- "Enabling Encryption Between the Web Client Browser and Web Server" on page 3-14
- "Enabling Encryption Between the Web Server and Siebel Server" on page 3-14
- "Enabling Encryption for Security Adapters" on page 3-14
- "About Using TLS with Siebel Enterprise Application Integration (EAI)" on page 3-14
- "Securing the Siebel Web Server" on page 3-15
- "Securing the Siebel Server" on page 3-18
- "Securing the Siebel Client" on page 3-19
- "Securing Email Communications" on page 3-25

For additional information, see *Siebel Security Guide* which includes information about communications and data encryption, security adapter authentication, and SWSE security features. For more information on the support for TLS encryption provided by Siebel CRM, see 1944467.1 (Article ID) on My Oracle Support.

Note: To ensure that you are using the highest level of security, download and install the latest Innovation Pack and patchset release to enable the highest level of security and obtain the latest security-related patches. For more information on this, see *Siebel Installation Guide* for the operating system you are using and *Siebel Patchset Installation Guide for Siebel CRM* (1614310.1 Article ID on My Oracle Support).

3

Securing the Network and Infrastructure

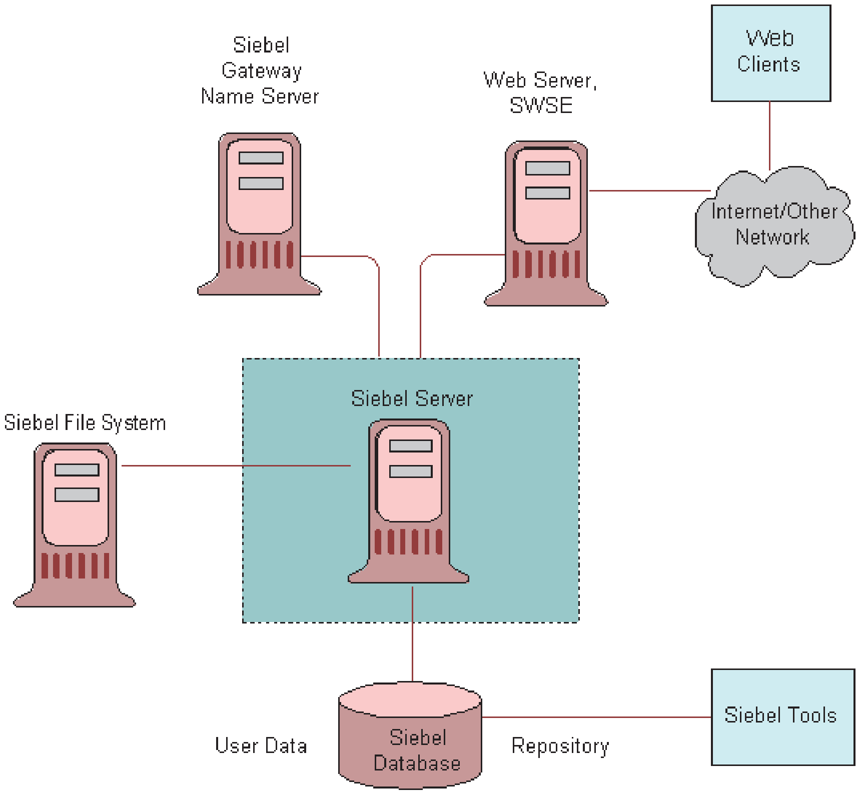
This chapter describes how to secure your network infrastructure and outlines the minimum network configurations. It includes the following topics:

About Securing the Network Infrastructure

Where and how network computing resources reside, as well as how they work in connection with the Internet and other computers on the local network, can have a significant impact on network security. This topic describes the network components to consider in securing your Siebel Business Applications deployment. You must consider the physical layout of the network components and the network authentication measures required.

Figure 3–1 shows the basic components included in Oracle's Siebel Business Applications network.

Figure 3–1 Siebel Network Components



Access to the devices that host Siebel Business Applications must be protected. If these devices are compromised, then the security of all applications on the computer is at risk. Utilities that provide computer-level security, for example, by enforcing computer passwords, can be used and are transparent to Siebel Business Applications.

Siebel Business Applications support the deployment of firewalls throughout the enterprise as well as reverse-proxy servers, Network Address Translation devices, and load balancers to secure the application from attack.

The architecture of Siebel Business Applications also takes advantage of high-availability technologies, such as Microsoft Cluster Services, which spread the workload across multiple computers allowing them to function as one. High-availability technologies address the need for failover and disaster-recovery management.

The following topics provide recommendations for deploying network components in securing your Siebel Business Applications infrastructure:

- "Network Zones and Firewalls" on page 3-3
- "Guidelines for Assigning Ports on Firewalls" on page 3-4
- "Guidelines for Deploying Siebel Business Applications Across a Firewall" on page 3-5
- "Routers" on page 3-5
- "Network Address Translation" on page 3-5
- "Load Balancers" on page 3-5
- "Proxy Servers" on page 3-6

- "Virtual Private Networks" on page 3-7
- "About Using Internet Protocol Security" on page 3-8
- "Preventing Denial of Service Attacks" on page 3-8

> **Note:** Siebel Business Applications do not use Simple Network Management Protocol (SNMP) for managing network devices. You can disable Simple Network Management Protocol services on Siebel Servers, if required.

Network Zones and Firewalls

A firewall separates a company's external Siebel Web Clients (those accessing applications over the Internet) from its internal network and controls network traffic between the two domains. A firewall defines a focal point to keep unauthorized users out of a protected network, prohibits vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks.

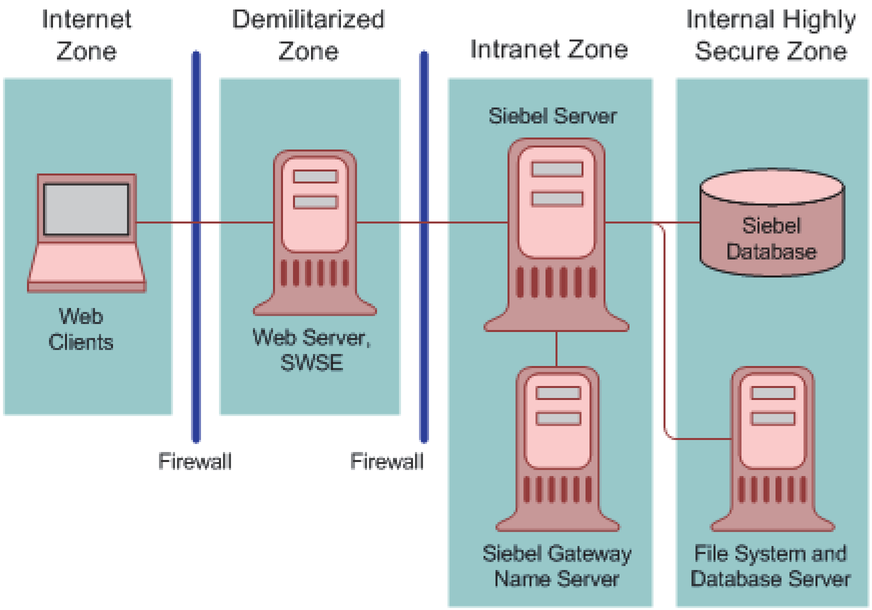
To secure a network, divide the network into zones of control by considering factors, such as the type of information contained in the zone and who needs access to that zone. Then place firewalls between the zones and implement access controls between the zones. As illustrated in Figure 3–2, "Recommended Firewall Deployment in a Siebel Business Applications Environment", an enterprise network for Siebel Business Applications typically comprises the following zones of control:

- **Internet zone.** This zone is insecure and not trusted. External Siebel Web Clients reside in this zone.
- **Demilitarized zone.** Publicly accessible servers are placed in this zone. Servers placed in this zone are called *bastion hosts.* Siebel Web servers and Web server load balancers reside in this zone. Clients outside the firewall access the Web server and the Siebel Server through a secure connection. This zone is where the external network first interacts with the Siebel environment.
- **Intranet zone.** This zone consists of internal networks.

  Components that reside inside this zone include Siebel Servers, the Siebel Gateway Name Server, a third-party HTTP load balancer (if deployed) for Siebel Servers, and the authentication server (Lightweight Directory Access Protocol or Active Directory Service Interfaces directory server). In a deployment of Siebel employee applications, internal Web clients can also reside in this zone.
- **Internal highly secure zone.** Business critical information and services are placed in this zone. The Siebel database and Siebel File System reside in this zone. Restrict access to this zone to system administrators and database administrators.

Figure 3–2, "Recommended Firewall Deployment in a Siebel Business Applications Environment" shows the recommended placement of firewalls in a Siebel Business Applications environment, that is, between the Internet and demilitarized zones, and between the demilitarized and intranet zones. For optimum performance, do not install a firewall between the intranet zone and the internal highly secure zone.

Figure 3–2 Recommended Firewall Deployment in a Siebel Business Applications Environment



For additional information on the recommended placement of firewalls, see "Recommended Network Topologies" on page 3-9. For information on assigning ports when setting up firewalls, see "Guidelines for Assigning Ports on Firewalls" on page 3-4.

Guidelines for Assigning Ports on Firewalls

This topic provides guidelines for assigning ports when setting up firewalls in a Siebel Business Applications implementation.

Configure communication ports as follows:

- Set up the external firewall to enable HTTP (default port 80) and HTTPS (default port 443) communications between external Siebel Web Clients in the Internet zone and the IP address of the Web server in the demilitarized zone according to the security parameters set on the Siebel Web Server Extension (SWSE).
- Set up the choke firewall (the firewall between the demilitarized zone and the intranet) as follows:
  - For communications from the Web servers to the Siebel Server, use the SCBroker port (Siebel load balancing) or the virtual port of a third-party HTTP load balancer for Transmission Control Protocol (TCP) traffic. The default port used by SCBroker is 2321.
  - For communications from the Web servers to the Gateway Name Server, enable port 2320.
- If you choose to place an internal firewall between the intranet zone and the internal highly secure zone, then set up the internal firewall as follows:
  - Enable port 636 for secure transmission of authentication information between the security adapter and the Siebel Servers. (The default is port 389.)
  - For communications between the Siebel Server and the Siebel database, enable the following default TCP ports:

    - 1433 (Microsoft SQL)
    - 1521 (Oracle)
    - 50000 (DB2)
  - (Microsoft SQL only) Enable TCP port 139 and UDP ports 137 and 138 for communications between the Siebel Server and the Siebel File System.

For additional information on the default port allocations used by Siebel Business Applications, see Appendix B, "Default Port Allocations." For additional information on firewalls, see "Network Zones and Firewalls" on page 3-3.

Guidelines for Deploying Siebel Business Applications Across a Firewall

When deploying Siebel Business Applications across a firewall, verify that your firewall and proxy servers support the HTTP 1.1 protocol. This protocol enables functionality, such as inline data compression to improve performance for bandwidth-constrained environments, cookies, and other features.

If your firewall does not support HTTP 1.1, and you use HTTP 1.0 instead, then lower performance will result. The following requirements apply if you do not use HTTP 1.1:

- Web server compression for SWSE must be disabled. In the eapps.cfg file, set the value of the DoCompression parameter to `FALSE`. (Use other settings where compression is known to be supported, or might be supported.) For more information, see *Siebel System Administration Guide*.
- Make sure that the firewall can handle cookie-wrapping or other proxy-specific features that enable forwarding of a cookie. Or, reduce or remove the use of cookies in your Siebel Business Applications. For more information, see *Siebel Security Guide*.
- Make sure that your proxy server does not pass to the SWSE any header content that uses HTTP 1.1 protocol. The proxy must remove any header content that is not compliant with HTTP 1.0.

Routers

Set up a screening router that selectively blocks or allows packets destined for internal resources. The screening router is typically a gateway to the external world, which is located at the perimeter, and is set up with the appropriate access list.

Network Address Translation

Network Address Translation rewrites the IP addresses of Internet connections as they cross the firewall boundary, thereby preventing direct access between the internal network and external networks, such as the Internet and partner networks.

Implement Network Address Translation on zone border security devices between the Web client and the Web server, and between the Web server and the Siebel Server.

Load Balancers

You can balance loads on your Siebel Servers using native Siebel load balancing or a third-party HTTP load balancer. Using HTTP load balancing distributes incoming network traffic over several servers.

A third-party load balancer typically can provide additional security features, such as limiting TCP port exposure to a single port for multiple Siebel Servers. Single-port exposure allows you to consolidate network access for better port monitoring and security. It also provides simplified firewall configuration. You have to configure only one virtual port.

Additional security features provided by most third-party load balancers include:

- **Denial of service (DoS) attack prevention.** In a DoS attack, a third-party HTTP load balancer helps handle the TCP connections. Incoming attacks can be caught at the load balancer before they reach the Siebel Server. A third-party HTTP load balancer typically has a built-in mechanism to stop DoS attacks at the point of entry.
- **Virtual Internet Protocol (VIP) addressing.** A third-party HTTP load balancer uses VIP addressing. Unlike an IP address, a VIP address is not associated with a specific device in a network, so VIP addressing helps prevent hackers from accessing Siebel Servers directly. Web servers in the demilitarized zone communicate with the VIP only.
- **TCP handshake protection.** The TCP handshake is replayed from the third-party HTTP load balancer to the Siebel Server rather than directly from the Web server in the demilitarized zone to the Siebel Server. This helps prevent attacks in which the TCP handshake is intercepted and redirected, for example, a SYN flood DoS attack.

When installing Siebel Business Applications, if you are using Siebel Server or third-party HTTP load balancers, then plan the use of TCP ports for firewall access:

- If Siebel load balancing is used, then make sure the Web server can access the SCBroker port on each Siebel server.
- If a third-party load balancer is used, then make sure the Web server can communicate with the VIP addresses and ports specified in the load balancer.

For information on the default port allocations used by Siebel Business Applications, see Appendix B, "Default Port Allocations."

Proxy Servers

Siebel Business Applications support the use of both forward and reverse-proxy servers within a deployment. Using proxy servers enhances security by preventing direct access to servers from the Internet.

Forward Proxy Servers

Forward proxy servers are generally used to provide Web access to the Internet for client computers when direct routing is not possible, either because it is forbidden by policy or by the network implementation. Forward proxy servers are therefore part of the client security infrastructure. They are also sometimes used by Internet service providers for caching.

Reverse Proxy Servers

A reverse-proxy server acts as an intermediary to prevent direct connections from clients to Web servers. A reverse-proxy server shields internal IP addresses from users by rewriting the IP addresses of the Web servers so that the Web server IP addresses are not revealed to the user. Additionally, the reverse proxy server can cache data closer to end users, thereby improving performance. Reverse-proxy servers provide an additional layer of security by helping protect the Web server from direct external attacks, but do not directly help secure the Web application.

To handle traffic between the external Siebel Web clients and the Web server that contains the SWSE, install a reverse-proxy server in the demilitarized zone (see Figure 3–2, "Recommended Firewall Deployment in a Siebel Business Applications Environment"S). The Web server and SWSE can then be moved behind a firewall into a separate zone or into the intranet zone.

Customer applications, which use standard interactivity, commonly are deployed with reverse proxy servers. Employee applications, which use high interactivity or Siebel Open UI, can also be deployed with reverse proxy servers. If you deploy applications that use high interactivity or Siebel Open UI with a reverse proxy server or a Web server load balancer, then note the following considerations:

- Siebel Business Applications do not support the translation of port numbers or protocol switching. An example of protocol switching is changing from HTTP to HTTPS.

  > **Note:** Protocol switching from HTTPS to HTTP is supported if you have enabled the TLS acceleration feature for communications between Siebel Web Clients and the Web server. For information on using TLS acceleration, see *Siebel Security Guide*.

- Siebel Business Applications support rewriting of the host name and of the IP addresses of the Web servers. For example, you can rewrite the following URL:

  ```
  http://ServerInternal/callcenter_enu/start.swe
  ```

  to:

  ```
  http://ServerExternal/callcenter_enu/start.swe
  ```

  However, you cannot rewrite it to:

  ```
  http://ServerExternal/portal1/start.swe
  ```

- The reverse proxy server and Web server must run on the same port.
- If you deploy Transport Layer Security (TLS) between the client and the reverse proxy server, then you must also deploy it between the reverse proxy server and the Web server on which the Siebel Web Server Extension (SWSE) is installed. Similarly, if you deploy TLS between the reverse proxy server and the Web server, then you must deploy it between the client and the reverse proxy server.

  > **Note:** If the TLS acceleration feature is enabled, then you can deploy TLS between Siebel Web Clients and the reverse proxy server. However, you do not have to deploy TLS between the reverse proxy server and the Web server. You can use the HTTP protocol for communications between the reverse proxy server and the Web server. For information on enabling TSL acceleration, see *Siebel Security Guide*.

Virtual Private Networks

Siebel Business Applications also support the use of Virtual Private Networks (VPNs). A VPN is a technique that allows computers outside the firewall to tunnel traffic through a firewall and to appear as if they are connected inside the firewall.

VPN technology allows employees working remotely to access many corporate intranet resources (for example, email servers, file shares, and so on) which are otherwise not sufficiently secure to be placed outside the firewall.

About Using Internet Protocol Security

Internet Protocol Security (IPsec) is a mechanism for securing communications at the Internet Protocol (IP) layer. If IPsec is implemented, then IP packets (including the TCP information) are encrypted. You do not have to configure Siebel Business Applications to enable IPsec in your deployment.

IPsec encrypts TCP data; that is, data at layers 4 to 7 of the OSI model. If you want to implement load balancing, then be aware that Web server load balancers cannot balance loads for encrypted information from layers 4 to 7. Before implementing IPsec, therefore, check with the server load-balancing vendor for support details.

If you implement IPsec, then follow these recommendations:

- Enable port 500 (User Datagram Protocol) and the IP protocols 50 and 51 on the perimeter firewall for IPsec communications.
- It is recommended that you enable pass-through authentication on the VPN Gateway to support Network Address Translation on the client side. (The VPN Gateway can be the firewall with VPN functionality or a separate VPN server behind the firewall).

Preventing Denial of Service Attacks

Denial of service (DoS) attacks can take different forms. However, the most common method involves one or more computers (often hijacked personal computers) bombarding a Web site or Web-accessible service with a large number of simultaneous requests. The affected servers are overwhelmed and the connections and processes are prevented from running. These types of attacks are almost always targeted against public-facing Web sites and applications.

The following steps can help prevent DoS attacks from affecting your employee-facing Siebel Business Applications:

- Use different Web servers for public-facing applications and for employee-facing applications so that even if the public Web servers are overwhelmed, Web servers are still available to service employee applications. For additional information, see "Proxy Servers" on page 3-6.
- Run the employee-facing Application Object Managers and key components on different Siebel servers from those used to run public-facing Application Object Managers. This step helps to make sure that even if the Siebel Servers that process external applications are overwhelmed with requests, hardware resources are available to continue processing internal applications. For additional information, see "Load Balancers" on page 3-5.

Other methods available when configuring firewalls to assist in preventing DoS attacks include designing them to reject rapid requests from the same IP address, or to blacklist specific IP addresses or domains. These methods are not foolproof and it might not be possible to use blacklisting on large public sites. For example, many DoS attacks use hijacked computers that are on large, well-known, Internet service providers. Blacklisting all of the users in these domains or IP ranges helps prevent the DoS attacks, but possibly prevents many valid users from using your Web site as well.

Recommended Network Topologies

This topic describes the recommended topologies for two different deployments of Siebel Business Applications:

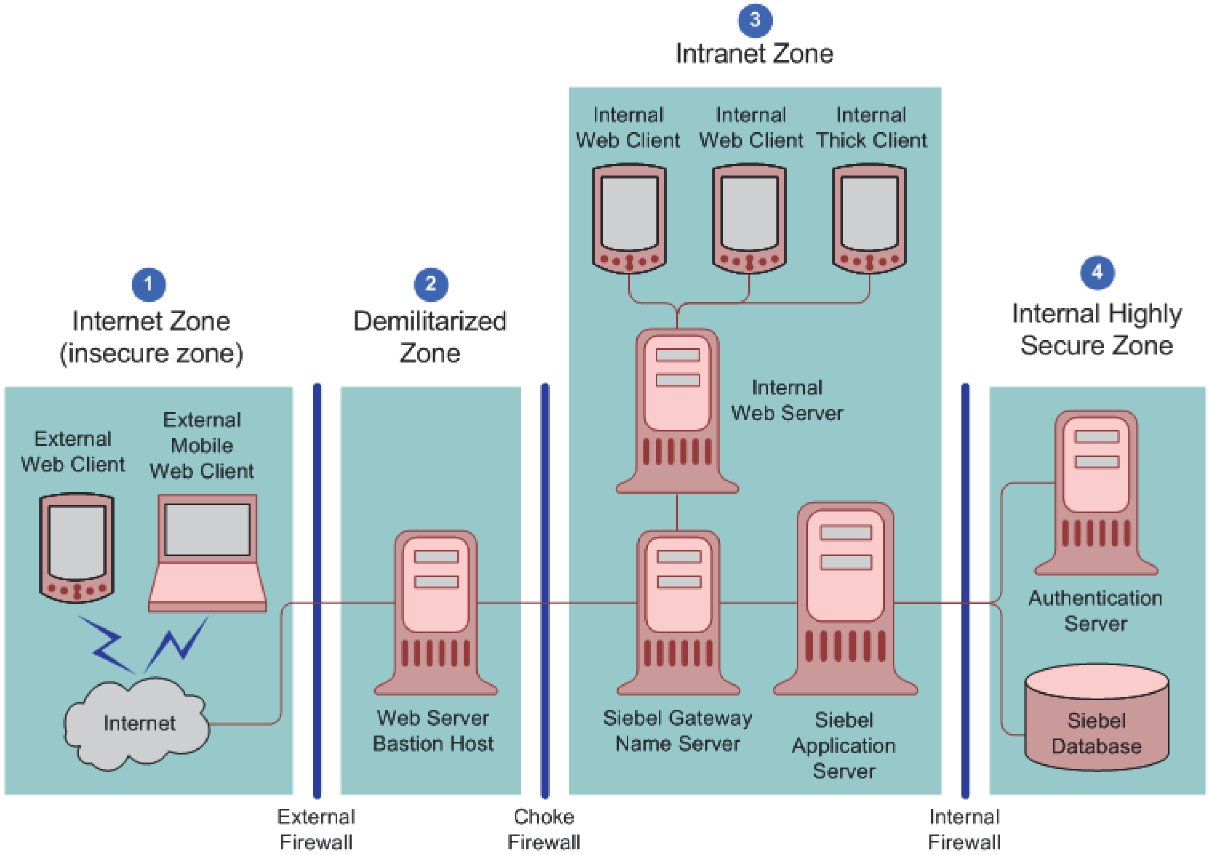
- A medium-scale, secure deployment of Siebel Business Applications with internal and external users
- A large-scale, secure deployment of Siebel Business Applications with internal and external users where high-availability is crucial

Network Configuration for Medium-Scale Deployments of Siebel Business Applications

Figure 3–3, "Network Configuration for a Medium-Scale Secure Deployment of Siebel Business Applications"shows the recommended placement of firewalls and related Siebel Enterprise Server components in a small or medium-scale Siebel Business Applications deployment with internal and external users. The Siebel network configuration for a medium-scale secure deployment is as follows:

1. **Internet zone.** External Siebel Web clients residing in the Internet zone access the Web server placed in the demilitarized zone through the external firewall.
2. **Demilitarized zone.** The Web server in this zone hosts a proxy server. The firewall keeps unauthorized users out of the protected network and the proxy server provides protection from various kinds of IP spoofing and routing attacks.
3. **Intranet zone.** The Siebel Web Server Extension (SWSE) is installed on the internal Web server in the intranet zone. The Siebel Gateway Name Server, Siebel Servers, and the third-party HTTP load balancer (if deployed) are also placed in the intranet zone.
4. **Internal highly secure zone.** This zone contains the Siebel database, Siebel File System, database server, and the authentication server (a Lightweight Directory Access Protocol (LDAP) server or Active Directory server). Limit access to this zone to authorized system administrators and database administrators.

Figure 3–3 Network Configuration for a Medium-Scale Secure Deployment of Siebel Business Applications



The network configuration approach illustrated in Figure 3–3 follows a defense-in-depth strategy by placing firewalls between the zones of control with only appropriate ports open. A secure channel is implemented using Transport Layer Security (TLS) between the external Web clients and the Web server to take care of security in the insecure Internet.

Network Configuration for Large-Scale Siebel Deployments

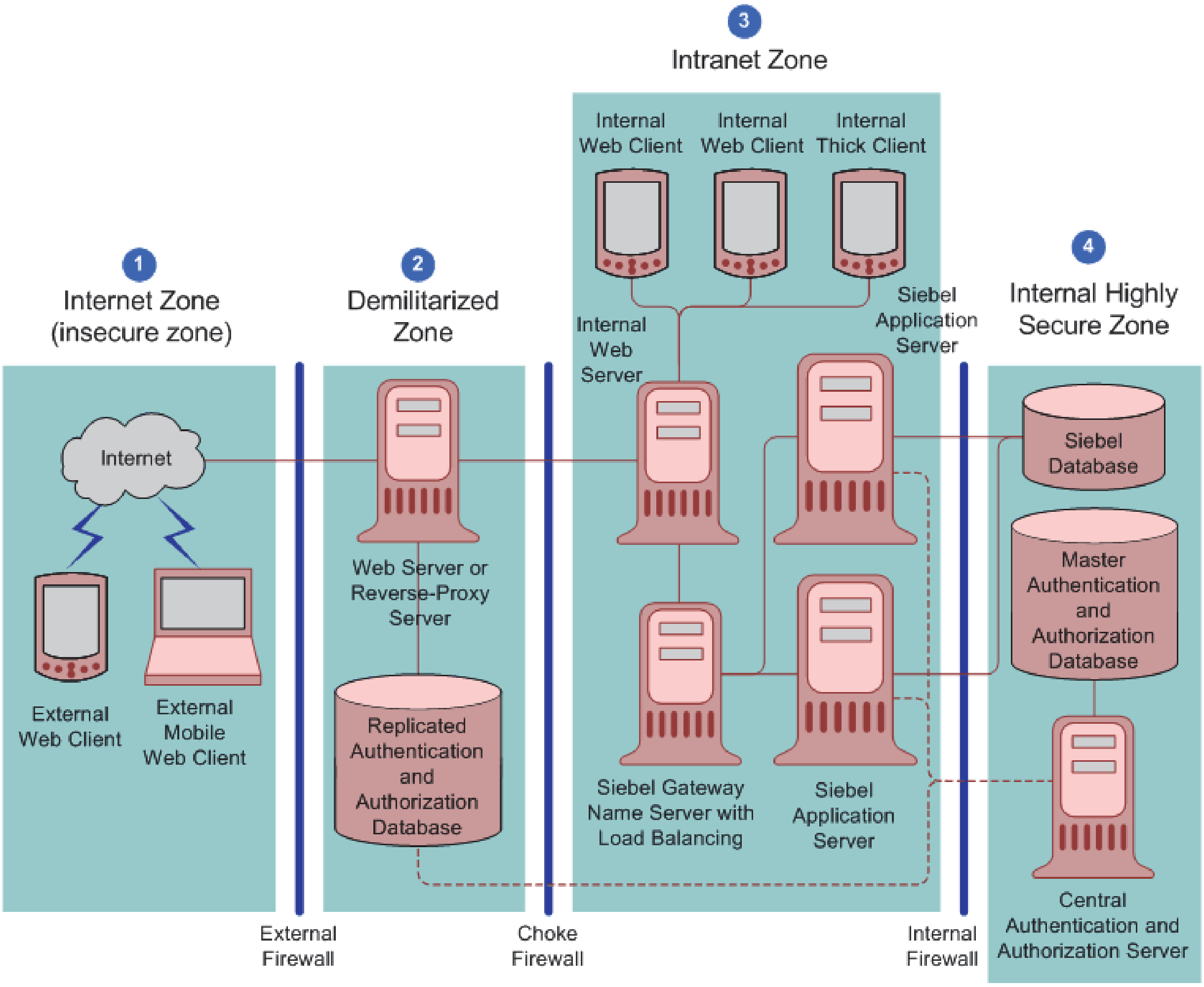
Figure 3–4, "Large Scale Highly Secure Deployment of Siebel Business Applications" shows the recommended placement of firewalls and related Siebel Enterprise Server components in a large-scale, secure Siebel Business Applications deployment with internal and external users. The Siebel network configuration for a large-scale secure deployment is as follows:

1. **Internet zone.** External Siebel Web clients residing in the Internet zone access the Web server placed in the demilitarized zone through the external firewall.
2. **Demilitarized zone.** A reverse-proxy server is included as a front end to the external Siebel Web clients to provide an extra layer of security in the demilitarized zone. The reverse-proxy server safeguards the Web server and the Siebel Servers. It acts as an intermediary to prevent direct connections from clients to Web servers, and it prevents the IP addresses of Web servers being revealed to the external world.
3. **Intranet zone.** The Web server, Siebel Gateway Name Server, and the Siebel Servers are placed inside the intranet zone. Siebel load balancing or third-party

HTTP load balancing is implemented to distribute the processing load to multiple Siebel Servers.

4. **Internal highly secure zone.** The Siebel database, Siebel File System, database server, central authentication and authorization server, and the master authentication or authorization database server (LDAP or Active Directory server) are placed in the internal highly secure zone. They contain confidential data, with access limited to authorized system administrators and database administrators only.

Figure 3–4 Large Scale Highly Secure Deployment of Siebel Business Applications


3
Intranet Zone
Internal Web Client
Internal Web Client
Internal Thick Client
1
Internet Zone (insecure zone)
2
Demilitarized Zone
Internal Web Server
Siebel Application Server
4
Internal Highly Secure Zone
Internet
Siebel Database
Master Authentication and Authorization Database
Web Server or Reverse-Proxy Server
External Web Client
External Mobile Web Client
Replicated Authentication and Authorization Database
Siebel Gateway Name Server with Load Balancing
Siebel Application Server
Central Authentication and Authorization Server
External Firewall
Choke Firewall
Internal Firewall

If you are using a centralized authentication and authorization system, then it is recommended to put a read-only replica of the authentication and authorization information in a database close to the reverse-proxy server in the demilitarized zone. (Determine whether or not to make a copy of the authentication database available in the demilitarized zone according to the sensitivity of your data.) Encrypt communications and information between the reverse-proxy server and the authentication database.

Using a replica database of the authentication information reduces the amount of traffic and firewall rules between the reverse-proxy server and the internal authentication and authorization servers. The centralized authentication system pushes the policies and rules to the replica database, and then the reverse-proxy server communicates with it. Although this type of configuration does not improve security, it improves application availability and performance. Availability is considered a part of security.

Network Authentication and Monitoring

The following authentication practices are recommended to secure your network:

- Maintain and implement authentication information centrally in a Web single sign-on (SSO) environment, then copy the information to the demilitarized zone. It is recommended that the authentication information in the demilitarized zone is read-only, is encrypted while stored, and is encrypted when transferred between the authentication database and other components.
- Maintain access to the internal resources from any external network on the least-privilege principle to protect the internal network from being compromised.
- Allow services through the firewall only from specific IP addresses to specific IP addresses, depending on the business requirement.
- Deploy network-based Intrusion Detection Systems (IDS) in stealth mode within the zones of control, and restrict access to log files and to methods of setting log levels so that intruders cannot cover their tracks.

  Network-based IDS can be deployed to provide identification and notification capabilities and can be used to complement firewalls in thwarting attacks. Implement a real-time monitoring mechanism to react to any critical penetration attempts in a timely manner.
- Setup and maintain host-based IDS on bastion hosts (for example, email relay) with appropriate monitoring mechanisms in place to react to access violations. Deploy host-based IDS on all key computers to defend against common and company-specific violations from insiders and outsiders. Host-based IDS can help with monitoring and reporting user and network activity, auditing system configurations and vulnerabilities, checking file integrity, recognizing attack patterns, and auditing user activity for policy violations.
- Use scanning tools to find common security violations.
- Add all networking patches.
- Enable auditing and track users’ login activity.

  For information on configuring and using Siebel Audit Trail, see *Siebel Applications Administration Guide* and "Implementing Auditing" on page 7-1.

Enabling Encryption of Network Traffic

If a Siebel Business Applications deployment over the Internet does not implement encryption between users' browsers and the Web server or between the Web server and application server, then such a deployment is susceptible to network sniffing and compromising of sensitive data. Implementing encryption for all network traffic and for all sensitive data prevents network sniffing attacks.

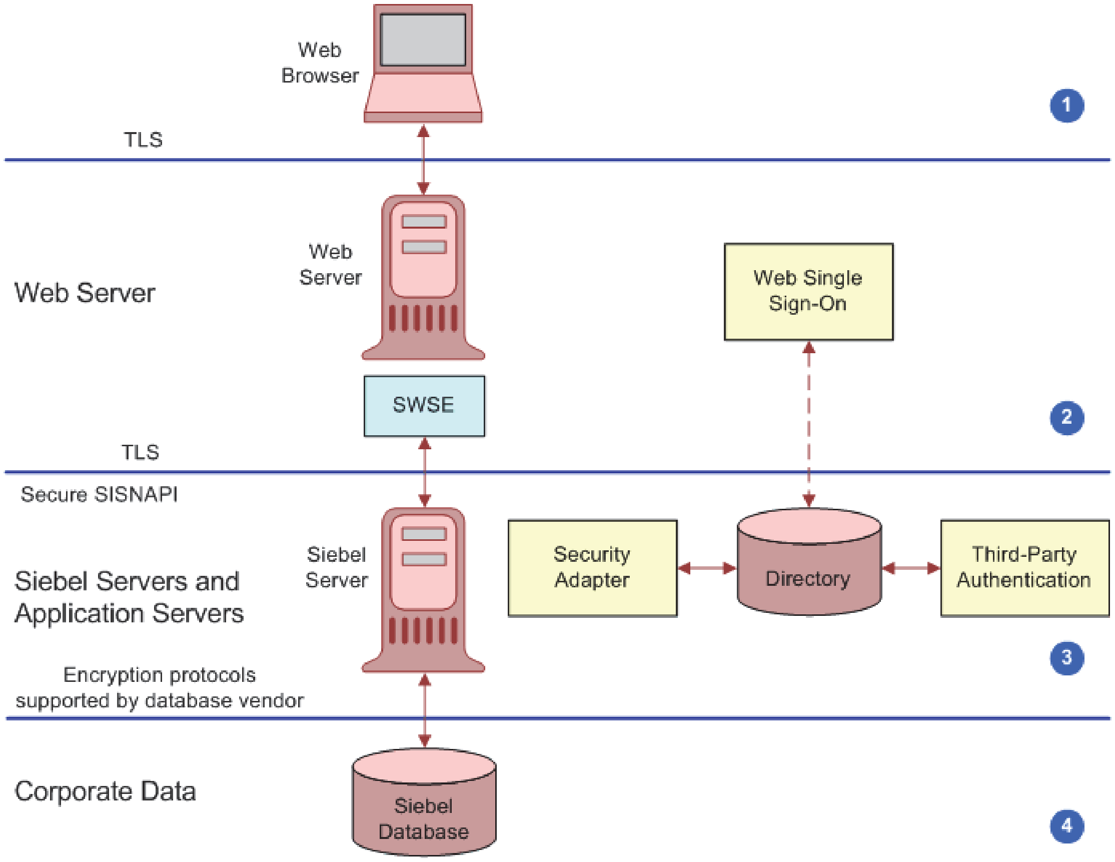
In Siebel Business Applications, stored data can be selectively encrypted at the field level, and access to this data can be secured. In addition, data can be converted into an encrypted form for transmission over a network. Encrypting communications safeguards such data from unauthorized access.

As illustrated in Figure 3–5, encryption protects confidentiality along the entire data communications path, from the Web client browser to the Web server, to the Siebel

Server, and back again. It is recommended that TLS encryption is enabled where possible. Figure 3–5 shows the types of encryption available for communications within the Siebel environment. Communications encryption is available in the following areas:

- Between client browser to Web server
- Between Web server to Siebel Server
- Between Siebel Server to database
- For database storage

Figure 3–5 Encryption of Communications in the Siebel Business Applications Environment



For additional information on encryption options available, see the following topics:

- "Enabling Encryption Between the Web Client Browser and Web Server" on page 3-14
- "Enabling Encryption Between the Web Server and Siebel Server" on page 3-14
- "Enabling Encryption Between the Siebel Server and Siebel Database" on page 3-14
- "Enabling Encryption for Security Adapters" on page 3-14
- "About Using TLS with Siebel Enterprise Application Integration (EAI)" on page 3-14

Enabling Encryption Between the Web Client Browser and Web Server

Siebel Business Applications run using the Siebel Web Client in a standard Web browser. When a user accesses a Siebel application, a Web session is set up between the browser and the Siebel Server, with the Web server in between. To protect against session hijacking when sensitive data is transmitted, it is recommended that you use the TLS protocol for communications between the browser and Web server, if support for this protocol is provided by your Web server.

The use of TLS for Web server and Siebel Web Client communications is transparent to Siebel Business Applications. For information on configuring TLS for Web server communications with the browser, see the vendor documentation.

You can specify the Web pages (known as views) within a Siebel application that are to use TLS. For additional information, see "Setting Security Features of the Siebel Web Server Extension" on page 3-17.

Enabling Encryption Between the Web Server and Siebel Server

Siebel Business Applications components communicate over the network using a Siebel TCP/IP-based protocol called SISNAPI (Siebel Internet Session API). You have the option to secure SISNAPI using TLS or embedded encryption from RSA or Microsoft Crypto APIs. These technologies allow data to be transmitted securely between the Web server and the Siebel Server. For additional information, see *Siebel Security Guide*.

Enabling Encryption Between the Siebel Server and Siebel Database

For secure transmission between the Siebel database and the Siebel Server, data can be encrypted using the proprietary security protocols specific to the database in use. For additional information, see your RDBMS vendor documentation.

Enabling Encryption for Security Adapters

You can implement TLS encryption for connections between a Siebel LDAP or ADSI security adapter and a certified LDAP directory or Active Directory. By enabling encryption for the Siebel security adapter, a secure connection is established between the Siebel application and the directory server.

The procedure for implementing encryption for a security adapter varies according to the type of security adapter you implement. The following parameters must be set:

- To configure encryption for the LDAP security adapter, set the SslDatabase parameter value for the LDAP Security Adapter profile or named subsystem to the absolute path of the Oracle wallet directory.
- To configure encryption (TSL) for the ADSI security adapter, set the parameter UseSsl to a value of True for the ADSI Security Adapter profile or named subsystem.

For detailed information on implementing communications encryption for a security adapter, see the topics about installing LDAP client software and process of installing and configuring LDAP client software in *Siebel Security Guide*.

About Using TLS with Siebel Enterprise Application Integration (EAI)

It is recommended that Siebel Business Applications external interfaces (EAI), which use Web services to send and receive messages over HTTP, encrypt communications using the TSL protocol.

The Siebel EAI HTTP Transport business service lets you send XML messages over HTTP to a target URL (Web site) and uses the Siebel Web Engine (SWE) to provide inbound messaging from an application that uses HTTP.

For outbound messages, Siebel CRM supports client authentication for TLS-based communications (mutual authentication) using the EAI HTTP Transport business service. For information on configuring mutual authentication, see *Transports and Interfaces: Siebel Enterprise Application Integration* and *Siebel Security Guide*.

To enable TSL for inbound messaging using the EAI HTTP Transport business service, follow the steps in *Siebel Security Guide* that describe how to configure a Siebel Web Client to use TLS.

Securing the Siebel Web Server

Because a Web server is one of the most exposed and intruder-targeted elements in a network, securing the Web server is a priority. Before using your Web server in a Siebel Business Applications deployment, secure your Web server by applying vendor-recommended security procedures and practices as described in your Web server documentation. Then consider implementing the recommendations outlined in this topic.

Implementing a Proxy Server

Deploy a reverse-proxy server in the demilitarized zone to protect the Web server from attacks relating to denial of service and directory traversal. For additional information, see "Proxy Servers" on page 3-6.

Monitoring Disk Space

Monitor the disk space available on your Siebel Web server. If the Web server is allowed to reach the disk space limit, then denial of service events can occur when the Siebel Server or Siebel Web clients connect to the Siebel Web server. For information on the tools that are available to monitor disk utilization for your Web server, see your Web server vendor documentation. For additional information on denial of service attacks, see "Preventing Denial of Service Attacks" on page 3-8.

Removing Unnecessary Subdirectories (Windows)

See the vendor-specific security documentation for information on removing unnecessary subdirectories in a Windows environment.

Assigning Web Server File Permissions (Windows)

Set Web server file and directory permissions appropriately to make sure only authorized users can access and modify designated files. Siebel Web Server Extension (SWSE) directories contain executable files which must be protected, for example, Java scripts (.js files), cascading style sheets (.css files), and ActiveX controls (.cab files).

Use the following procedure to assign Web server file permissions in a Windows environment.

To assign Web server file permissions in a Windows environment

1. Start the IIS Manager Console.
2. Navigate to Start, Programs, Administrative Tools, and then choose the Internet Information Services (IIS) Manager.

3. Expand IIS, Local Computer, Web Sites, and then Default Web Site node.
4. Select a Siebel application, for example, callcenter_enu.
5. Right-click the Siebel application, then select Permissions.
6. Assign read and execute permissions for authorized users.
7. Verify that only authorized users have appropriate permissions on the SWSE files and directories.

Note: Administrators must have full rights to the Web server files and directories to grant and revoke permissions and to back up or recover tasks.

Encrypting Communications to the Web Server

It is recommended that you secure all communications between the Siebel Web Client, the Web server and the Siebel Server using TLS. For additional information on encrypting communications, see "Enabling Encryption of Network Traffic" on page 3-12.

Encrypting Passwords in the eapps.cfg File

The eapps.cfg file contains parameters that control interactions between the Siebel Web Engine and the Siebel Web Server Extension (SWSE) for all Siebel Business Applications. Passwords are written to the file in encrypted form when you initially configure the SWSE. Thereafter, encryption behavior is subject to the status of the EncryptedPassword parameter. The default value of the parameter is True. If the EncryptedPassword parameter does not exist in the eapps.cfg file, then the default behavior is the same as if EncryptedPassword is set to False. It is recommended that you verify that the EncryptedPassword parameter exists, and that it is set to True.

Note: If the EncryptedPassword parameter is set to True, then make sure that all passwords stored in the eapps.cfg file are encrypted.

If you manually edit the eapps.cfg file to set the EncryptedPassword parameter to True, then use the encryptstring utility to generate an encrypted version of the password to store in the file. For information on editing the eapps.cfg file and using the encryptstring utility, see *Siebel Security Guide*.

Securing User Session IDs

Session ID spoofing is a form of computer network attack during which a user’s session ID is intercepted during communications between a valid user's browser and the Web server. The attacker can then hijack that user's session by sending the still active Session ID in the URL with a SWE message back to the Web server.

Implementing TLS for communications between the client browser and the Web server helps reduce the risk of session ID spoofing. In addition, it is recommended that you perform the following steps:

- Enforce the use of session cookies to manage user sessions for Siebel Web Client users instead of allowing the session ID to be passed in the URL.

In cookieless mode, a user name and unencrypted password are also passed in the URL, which constitutes another possible security vulnerability and is an additional reason for enforcing the use of session cookies.

In some circumstances, it is not possible to use cookies, for example, if Siebel Business Applications are running inside a portal, or if an application, such as Oracle Business Intelligence Publisher (Oracle BI Publisher), is running from inside Siebel Business Applications. However, if you have implemented Web Single Sign-On as your method of user authentication, then for security reasons, it is recommended that you use cookie mode.

Note: Siebel Open UI clients do not support cookieless mode.

- Configure the Web server to encrypt the session ID in session cookies; this prevents unauthorized attackers from capturing the cookie and determining the format.

To secure session IDs by enabling the use of session cookies, perform the following procedure.

To secure user session IDs

1. To force the SWSE to always use cookie-based mode, edit the eapps.cfg file and add the following parameters:

```
SessionTracking = Cookie
URLSession = FALSE
CookieSession = TRUE
```

2. To configure the Web server to encrypt the session ID, edit the eapps.cfg file, and add the following parameter to the Defaults section:

```
EncryptSessionId = TRUE
```

Setting Security Features of the Siebel Web Server Extension

The SWSE can be configured to allow only URLs that use TLS over HTTP (HTTPS protocol) to access views in a Siebel application or to transmit user credentials entered in a login form from the browser. It is recommended that you implement both of these features. You can choose to:

- Use HTTPS only on the login view (to protect password transmission).
- Use HTTPS for additional specified views.
- Use HTTPS for all views.

You can indicate whether or not the HTTPS protocol must be used to access a view by doing either or both of the following:

Securing Access to Views

- Setting the Secure property of a specific view to True to indicate that the HTTPS protocol must be used to access the view (applies to Siebel Business Applications using standard-interactivity mode only).
- Setting the SecureBrowse parameter to True to indicate that all views in the Siebel application must use HTTPS, regardless of how the secure attribute is set for individual views. Securing the entire user session in this way helps to prevent network-sniffing attacks.

Use Siebel Server Manager to specify a value for the SecureBrowse component parameter. For information on this task, see *Siebel Security Guide*.

Securing Login Information

- To secure login information, it is recommended that you configure the Siebel Web Engine to transmit user credentials entered in a login form from the browser to the Web server to use HTTPS. Securing login information prevents sniffing user credentials.
- To implement secure login, on each Siebel application where you want to implement secure login, set the value of the SecureLogin component parameter to True. For information on this task, see *Siebel Security Guide*.

Securing the Siebel Server

The following recommendations can enhance the security of your Siebel Servers.

Encrypting Communications to the Siebel Server

Enable encryption between the Web server and Siebel Server and between the Siebel Server and the Siebel database. For additional information on encrypting communications, see "Enabling Encryption of Network Traffic" on page 3-12.

Note: To disable specific ciphers in Siebel EAI in UNIX and Microsoft Windows, set the following in the mainwin or windows registry:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvid
ers\SCHANNEL\Ciphers]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvid
ers\SCHANNEL\Ciphers\cipher name]
"Enabled"=dword:00000000
```

Restricting Siebel Server Access

To restrict privileges to Siebel Server processes, assign an operating system account that is specific to the Siebel Server. Make sure this account has access only to files, processes, and executable files required by Siebel Business Applications.

- In Windows operating system environments, remove or limit the use of shared folders.
- In UNIX operating system environments:
  - Do not make the Siebel Server account the root administrator.
  - Disable UNIX r-services (for example, rlogin, rshell, rexec, rcp).

    R-services allow users to log in to and run various commands on a remote host computer. Before you can run the r-services on a remote host, you are required to provide authentication to access the host *unless* the local computer is listed in the .rhosts file, in which case authentication is not required. Therefore to provide the appropriate level of access and control to the Siebel Server, it is recommended that you disable the usage of r-services. Once you have disabled r-services, .rhosts files are not required and can be removed.

Encrypting the jndi.properties File

The user credentials in the jndi.properties file are stored in clear text format. To fix this, it is recommended that you encrypt the jndi.properties file as shown in the following procedure.

To encrypt the jndi.properties file

1. Set up the Siebel Server and the JMS server.
2. Create a named subsystem based on JMSSubsys.
3. Encrypt the jndi.properties file using the batch script files.

   Note the following:

   - The batch script files include the following: EncodeJndiProperties.sh, EncodeJndiProperties.bat, Siebel.jar, and ClientAppEAIJMSBsvDll.
   - The batch script files use the java-based encryption utility, com.siebel.eai.jms.EncodeJndiProperties, to encrypt the jndi.properties file and set the following properties in the JMSSubsys subsystem:
     - **JNDIEncryptionCheck.** Boolean value used to verify whether the jndi.properties file is encrypted (True) or not (False). The default value for JNDIEncryptionCheck is True.
     - **JNDIEncryptionSeed.** Seed value used to encrypt and decrypt the password.
   - The prerequisites for running the batch scripts include:
     - ***<JNDI file name>***. Full path to the jndi.properties file which is to be encrypted.
     - ***<Encryption seed>***. Encryption seed for encrypting the jndi.properties credentials.
     - ***<Gateway Server Name>.*** Gateway server name.
     - ***<Gateway Server Port>.*** Gateway server port.
     - ***<Siebel Enterprise>.*** Siebel enterprise name.
     - ***<Username>.*** Username to connect to the gateway server.
     - ***<Password>.*** Password to connect to the server.
     - ***<Name Subsystem>.*** The named subsystem to set the seed for decryption.
     - The batch scripts expect the user to set the SIEBEL_ROOT and JAVA_HOME environment variables.
4. Check the jndi.properties file to confirm that the password is actually encrypted.
5. To confirm that the setup works, use the Business Service simulator to run a test to set messages to the JMS server using the named subsystem created is Step 2.

Securing the Siebel Client

The following general guidelines are applicable for securing all client computers that access Siebel Business Applications. For specific information on security recommendations for mobile clients, see "Securing Mobile Clients" on page 3-21.

Deploying Siebel Open UI

You can optionally deploy Siebel Business Applications using the Siebel Open UI. Siebel Open UI is the most secure Siebel CRM client available and is therefore recommended if your Siebel implementation has high-security requirements.

Siebel Open UI has the following characteristics:

- Limited attack surface. Siebel Open UI uses only three technologies to render the client code: HTML, CSS, and JavaScript. Because of the small set of underlying technologies that are used to render the client and the absence of third-party plug-ins such as ActiveX and Java, Siebel Open UI provides the smallest possible attack surface.
- Transparent technology. Because the Siebel Open UI client is built entirely on standards, a variety of modern inspection tools can be used to validate the security compliance of your implementations.
- Compatibility with Data Execution Prevention features and virtualization. Because the Siebel Open UI client is a scripted client, it is fully compatible with Data Execution Prevention features for software or hardware, and compatible with virtualization features.
- Siebel Open UI clients enforce session security by requiring that session IDs can only be passed in session cookies. Passing session IDs through the URL (cookieless mode) is not secure and is not recommended for customer-facing deployments of Siebel Business Applications. Siebel Open UI clients do not support cookieless mode.

For additional information about Siebel Open UI, see *Deploying Siebel Open UI* and *Configuring Siebel Open UI*.

Enabling ActiveX Controls for High Interactivity Clients

Siebel Business Applications in high-interactivity mode use ActiveX technology to deliver several features, for example, email client integration. A browser running a high-interactivity application must be enabled to access and use ActiveX controls. You can do one of the following:

- Allow users to download ActiveX controls on demand from a Web server.

  This option is not preferred because it requires that users are assigned permissions associated with power users.
- Deploy the required ActiveX controls on users' computers (recommended option).

  If you deploy ActiveX controls on users' computers, then you can configure the client-browser settings to prevent additional ActiveX controls from being downloaded. For information on deploying ActiveX controls, see *Siebel System Administration Guide*.

If you are not using supported security-setting templates for applicable Web content zones for your Siebel Business Applications in high-interactivity mode, then to enable full functionality related to ActiveX controls you must manually enable the Internet Explorer ActiveX settings. For information on this task, see the chapter on configuring the browser for Siebel Web clients in *Siebel System Administration Guide*.

Encrypting Communications for Web Clients

It is recommended that you secure all communications between the Siebel Web Client and the Web server using TLS, if support for this protocol is provided by your Web server. Encryption is not set by default. For additional information, see "Enabling Encryption Between the Web Client Browser and Web Server" on page 3-14.

Providing Physical Security for the Client Device

The physical security of the client device is handled outside of Siebel Business Applications. You can use utilities that provide computer-level security by enforcing computer passwords or encrypting the computer hard drive. Most leading mobile devices have user-enabled passwords.

It is recommended that you use a two-factor authentication approach (for example, RSA Secure ID) for network components; this is a security process that confirms user identities using something users have and something they know. Requiring two different forms of electronic identification reduces the risk of fraud and protects against password attacks.

Defining a Policy for Unattended Personal Computer Sessions

Users should not leave workstations unattended while they are logged in to Siebel Business Applications; doing so makes their computer potentially accessible to unauthorized users. Define a corporate policy for handling unattended PC sessions. Oracle recommends using password-locked screen saver features on all PCs.

Keeping Browser Software Updated

Update browser software when new versions are released; new releases often include additional security features. If you are using Internet Explorer, then check the Microsoft Web site for the latest browser security patches.

Certain features and functions in Siebel Business Applications work in conjunction with security or other settings on the Web browser. Some of the security features provided by supported browsers and operating systems are not supported when used with Siebel Business Applications.

Detailed information about the browser settings used in deploying Siebel clients is provided in *Siebel System Administration Guide*. For more information about the settings in your Web browser, see the documentation that came with your browser.

Updating Security Patches

To protect against malicious software (malware), apply security patches provided by the desktop operating system provider on a regular basis. The same is true of patches released by antivirus software suppliers, and by companies that provide other third-party software products supported by Siebel Business Applications.

Securing Mobile Clients

Oracle provides a suite of mobile solutions that allow remote access to data within Siebel Business Applications. These solutions support a variety of mobile platforms, including smartphones, tablets, and laptop computers (running Siebel Mobile applications or Siebel Mobile Web Client). The following topics provide information about securing mobile devices running Siebel Business Applications:

- "Securing Siebel Remote" on page 3-22
- "Securing Mobile Devices Running Siebel Business Applications" on page 3-24

Securing Siebel Remote

Oracle's Siebel Remote enables a Siebel Mobile Web Client (MWC) that typically operates remotely in disconnected mode to connect to a Siebel Server so that the local client database can be synchronized with the enterprise Siebel database. Making the Siebel Remote architecture as secure as possible involves implementing security strategies for the following areas:

- "Securing the Synchronization Framework" on page 3-22
- "Encrypting Data in the Local Database and File System" on page 3-23
- "Defining Password Management Procedures" on page 3-24

Securing the Synchronization Framework

This topic outlines issues to consider and provides recommendations for securing the synchronization framework for Siebel Remote.

In addition to implementing the suggestions in this topic, make sure that you assign the least privileges required to the Siebel service owner account on the Siebel Server that runs the Synchronization Manager component. For additional information, see "Assigning Rights to the Siebel Service Owner Account" on page 4-7.

Authenticating the Mobile Web Client

By default, the Synchronization Manager does not authenticate incoming Remote client requests to make sure that the client is valid. It is recommended that you configure your Siebel application to require that client requests are authenticated by setting the value of the Authentication Method parameter of the Synchronization Manager to one of the supported authentication methods:

- Database
- LDAP
- Active Directory
- Siebel
- AppServer

The synchronization session takes place through a fixed port that is dedicated to the Synchronization Manager; the default TCP/IP port number is 40400. The port number is set on the Synchronization Manager Server component and is then open in any firewall. Therefore, it is recommended that you change the default value of the port.

Encrypting Communications

The synchronization session can be managed using unencrypted communications, but it is recommended that you implement RSA or MSCrypto encryption. To use encryption, both the Siebel Server and the Remote client must enforce encryption in their connection parameters. To enable encryption, set the Encryption Type parameter of the Synchronization Manager Server component to RSA or MSCrypto and change the DockConnString parameter in the [Local] section of the client .cfg file to the same value. For additional information, see *Siebel Remote and Replication Manager Administration Guide*.

Encrypting DX Transaction Files

Siebel Remote allows Mobile Web Clients to connect to a Siebel Server and exchange updated data and files during the synchronization process. The updated data is sent to or retrieved from the server in the form of .dx transaction files.

To protect your data, encrypt the .dx files using any suitable third-party utility, such as Pretty Good Privacy (PGP), when the files are removed from the `\docking` folder for any reason. To secure the .dx files within the `\docking` folder during run time, operating system-level encryption techniques can be used, for example, Microsoft Windows Encrypting File System, so that encryption and decryption are performed dynamically.

Caution: Implementing operating system-level encryption on the `\docking` folders can adversely affect data replication.

Using a VPN When Synchronizing Through the Internet

It is recommended that every synchronization session occur within the corporate firewall. If your deployment of Siebel Business Applications must support synchronization through the Internet from outside the firewall, then it is recommended that you use a Virtual Private Network (VPN).

If there is a firewall on the network between the synchronization client and the Siebel Server, or between the VPN server and the Siebel Server, then the port for synchronizing with the Siebel Server must be opened on the firewall, and this port must be a port other than port 80. If a VPN connection is not used, then it is possible that your Internet Service Provider (ISP) or another host on the route might block communications on this particular port. For additional information, see *Siebel Remote and Replication Manager Administration Guide*.

Encrypting Data in the Local Database and File System

The Siebel Mobile Web Client uses a local database to store data for user access and uses a local Siebel File System to store files. This topic outlines recommendations for securing both.

Local Database

Two local database template files are provided with Siebel Business Applications for use with Siebel Remote. These templates provide the starting point to generate your own database template:

- **sse_utf8.dbf.** A template that is not encrypted.
- **sse_encr.dbf.** A template that is encrypted with standard Sybase encryption.

By default, the template that defines the local database schema is not encrypted. It is recommended that you use the encrypted local database template to encrypt the entire local database, thereby providing a layer of security against unauthorized access to the local database.

To use an encrypted database template for mobile clients, the Generate New Database and Database Extract tasks must be configured and run using the sse_encr.dbf template. For information, see *Siebel Remote and Replication Manager Administration Guide*.

Local Siebel File System

If the local Siebel File System is used to store highly sensitive data, then it is recommended that you encrypt the local Siebel File System, either using third-party products or encryption features provided by your operating system.

Defining Password Management Procedures

When using the Siebel Mobile Web Client, secure access to the Siebel Server and to data on the local database by implementing password management procedures as follows:

- Implement the following password functionality for local database authentication provided by Siebel Business Applications:
  - Lock applications after a given number of failed-access attempts.
  - Disable passwords after a given period.
  - Check password formats based on specified rules.
  - Reset user passwords. The administrator performs this task.
- To guard against unauthorized administrative access to the local database, change the local database DBA password from the default value, which is the first eight characters of the Siebel Enterprise name.

  Specify a strong password for the local DBA by modifying the value of the New DBA Password parameter when generating a new database template.
- Enable password hashing. For information on this task, see "About Configuring Password Hashing for Users" on page 6-5.

Securing Mobile Devices Running Siebel Business Applications

Mobile devices must be secure. If a mobile device falls into the wrong hands, then organizations need assurance that sensitive data is not compromised. The following options are available for ensuring mobile-device security:

- Place the local database file on a secure digital card and encrypt the data. The encryption affects the performance of the mobile application. Remove the secure digital card when not in use, thereby securing the local database. Separating the secure digital card and the device prevents access to the local database.
- Secure the mobile device by setting an operating system-level password.

Siebel Business Applications provide a number of settings that can also be used to secure the mobile application:

- **Enable Application Lockout.** This allows the administrator to define a fixed number of login attempts that can be made before the Siebel application is locked for a specified period of time.
- **AllowRememberPassword.** If the AllowRememberPassword setting is set to False, then users cannot save their passwords to the device registry and must enter their passwords each time they log in.
- **Enable Encryption.** This setting stores the Siebel Mobile database in an encrypted form which cannot then be accessed outside of the Siebel Mobile application.

Securing the Siebel Document Server

Siebel Correspondence, Siebel Presentations, and Siebel Proposals all use the Siebel Document Server to generate Microsoft Word and Microsoft PowerPoint documents through the Web. All document templates come in through the Siebel Server. As such, the Siebel Server controls security and represents the only client that interacts directly with the Siebel Document Server. For more information about Siebel Document Server, see *Siebel Correspondence, Proposals, and Presentations Guide*.

Perform the steps in the following procedure to secure the Siebel Document Server.

To secure the Siebel Document Server

- Set up the appropriate permissions on the Siebel Document Server.

  It is recommended that only the user who authenticates as the Siebel service owner is given access to the Siebel File System and the ability to execute permissions on the Siebel Document Server. For additional information, see "Securing the Siebel File System" on page 4-3.

- Set a high-security level for macros.

  It is recommended that you set a high-security level for macros so that untrusted macros cannot be executed by the Siebel Document Server. This setting prevents the execution of malicious code in a document.

- Implement an antivirus policy.

  Make sure an antivirus policy is in place for computers that supply templates to the Siebel Document Server. By default, the operating system does not check for viruses or malicious code in a file. It is recommended that you check for viruses on all the templates that are submitted to the Siebel Document Server.

- Microsoft provides some standard utilities in the Resource kit to lock down security on a generic Microsoft Windows computer. It is recommended that tools, such as C2.exe be implemented to secure such an environment. These tools are readily available from Microsoft.

Securing Email Communications

This topic provides information on securing the Email server and email communications in a Siebel environment.

Siebel Email Response allows organizations to manage and respond to a large volume of incoming email. Siebel Email Response works in conjunction with the Siebel Communications Server and your third-party email server to process email. Both Siebel Email Response and Siebel Communications Server are installed with the Siebel Server.

The Siebel Communications Server uses communications driver files to communicate with the email system and to support inbound and outbound email processing. Oracle supports the Internet SMTP/POP3 Server and the Internet SMTP/IMAP Server for use with email servers that support the SMTP protocol for outbound email messages, or the POP3 or IMAP protocol for inbound email.

Implement the recommendations in the following topics to increase the security of your Siebel email environment:

- "Securing the Email Server" on page 3-26
- "Encrypting Communications Between the Siebel Server and the Email Server" on page 3-26

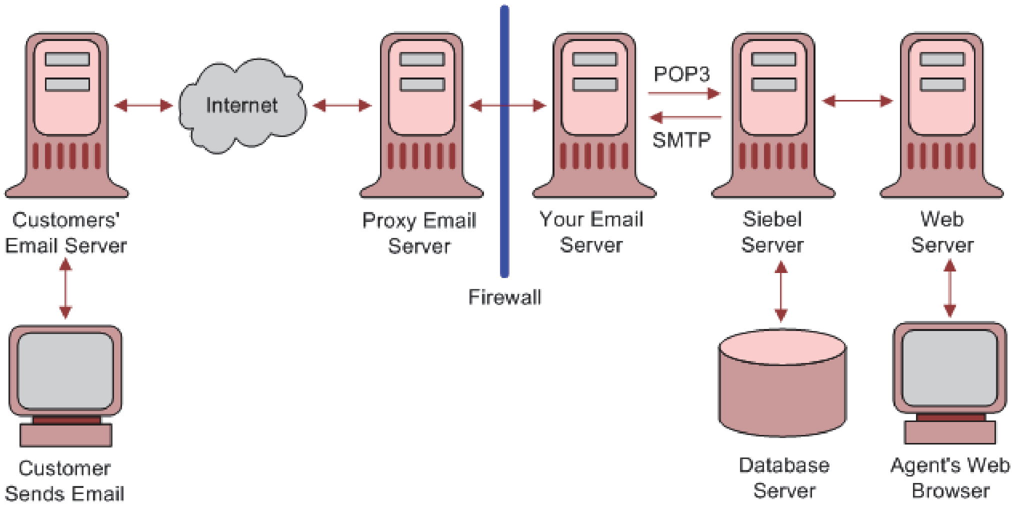
- "Deleting Processed Email Messages" on page 3-27

Securing the Email Server

The Siebel Email Response workflow begins when a customer sends an email to your company over the Internet. The email passes through the customer's email server and communicates with your email server, which receives the email and passes it to the Communications Inbound Receiver (CIR) on the Siebel Server.

To secure your environment, it is recommended that you deploy a proxy email server (SMTP Proxy) to process all incoming emails and a dedicated email server to process only the mailboxes used by Siebel Email Response on the Siebel Server. Figure 3–6 shows the recommended placement of email servers, with your Siebel Email Server secured behind the firewall.

Figure 3–6 Siebel Email Response Architecture Overview



Encrypting Communications Between the Siebel Server and the Email Server

The Siebel Communications Server uses the Internet SMTP/POP3 Server and the Internet SMTP/IMAP Server communications driver files to support Siebel email processing. Configuring parameters for the driver files allows you to determine email processing behavior for your environment.

To provide secure transmission of email data between the Siebel Server and the email servers, it is recommended that you enable TLS communications for SMTP, IMAP, and POP3 sessions. The following procedure describes how to enable a TLS connection for the Internet SMTP/POP3 or the SMTP/IMAP Server driver.

To enable TLS communications for SMTP, IMAP and POP3 sessions

1. Navigate to the Administration - Communications screen, then the Communications Drivers and Profiles view.
2. In the Communications Drivers list, select either the Internet SMTP/IMAP Server Driver or the Internet SMTP/POP3 Server Driver.
3. Click the Profiles view tab then, in the Profiles list, select the relevant profile.
4. In the Profile Parameter Overrides list, add new records as required for the following parameters and set the value of each to TRUE:

You can also enable a TLS connection for the Internet SMTP/POP3 or the SMTP/IMAP Server drivers provided you are using Microsoft Exchange Server 2007 or 2010 as your email server. Enable TLS using the following parameters:

- Enable TLS for IMAP
- Enable TLS for POP3
- Enable TLS for SMTP
- Enable TLS for Backup SMTP

For information on setting the SMTP/POP3 or SMTP/IMAP Server driver parameters to enable TLS, see *Siebel Email Administration Guide*.

Deleting Processed Email Messages

In a Siebel production environment, it is recommended that once incoming and outgoing email messages have been processed, they are deleted from the Siebel Server. The following parameters for the Internet SMTP/POP3 Server and the Internet SMTP/IMAP Server driver files determine whether or not messages are stored after processing:

- Delete Processed Messages

  Incoming email messages retrieved from the IMAP or POP3 server are saved to the Incoming Email directory as temporary files where they remain until they are processed. If you set the Delete Processed Messages parameter to TRUE (recommended), then the temporary files are deleted from the directory when the messages have been processed. If the Delete Processed Messages parameter is FALSE, then the processed temporary files are stored in the Processed Email directory.

- Save Sent Messages

  Whether or not copies of email messages that have been sent are saved on the Siebel Server is determined by the value set for the Save Sent Messages parameter. If the parameter is set to TRUE, then sent messages are saved to the Sent Email directory after processing. If the Save Sent Messages parameter is FALSE (recommended), then sent messages are not saved.

To prevent email messages from continuing to be stored on the Siebel Server after they have been processed, perform the steps in the following procedure.

To delete processed email messages

1. Navigate to the Administration - Communications screen, then the Communications Drivers and Profiles view.
2. In the Communications Drivers list, select either the Internet SMTP/IMAP Server Driver or the Internet SMTP/POP3 Server Driver.
3. Click the Profiles view tab and, in the Profiles list, select the profile you want to configure.
4. In the Profile Parameter Overrides list, add two new records using the values shown in the following table:

Name	Value
Delete Processed Messages	TRUE
Save Sent Messages	FALSE

For additional information on setting the SMTP/POP3 or SMTP/IMAP Server driver parameters, see *Siebel Email Administration Guide*.

Securing the Siebel Reports Environment

Siebel Business Applications use Oracle BI Publisher to generate Siebel reports. In a disconnected Siebel Reports environment, user authentication mechanisms are not required.

In the Siebel Reports connected environment, Oracle BI Publisher is installed separately from Siebel Business Applications and access to the BI Publisher Server is authenticated. To authenticate user access to the BI Publisher Server in a Siebel Reports connected environment, you can implement one of the following:

- **Siebel Security Model.** This model provides authentication using the EAI Application Object Manager.
- **LDAP security model.** This model provides authentication against a directory.

For information on the methods available to authenticate user access to the BI Publisher Server in a Siebel Reports connected environment, see *Siebel Reports Guide* and 1501378.1 (Article ID) on My Oracle Support.

Guidelines for Providing Additional Security for Oracle BI Publisher

To provide additional security for Oracle BI Publisher, the following steps are also recommended:

- **Change default ports to nonstandard ports.** As with other components, the Oracle BI Publisher installation is configured to run on a default set of ports.
- **Implement operating system-level encryption to dynamically encrypt Oracle BI Publisher configuration files.** Encrypting the configuration files protects them from being read by every user who has access to the BI Publisher Server.

4

Securing the Operating System

This chapter contains recommendations for securing your operating system. Securing your operating system contributes to the overall level of security that applies to your Siebel Business Applications. This chapter contains the following topics:

About Securing Operating Systems

Securing operating systems is the first step towards safeguarding the Siebel Business Applications deployment from intrusion. Workstations and servers are typically installed with a multitude of development tools and utilities. Securing an operating system involves the removal of all nonessential tools, utilities, and other system administration options. This process also requires that all appropriate security features are activated and configured correctly, and includes the following tasks:

- Protecting files and resources
- Restricting accounts and services to those who need them
- Applying and maintaining patches and product updates
- Performing maintenance activities, such as running security software

Note: Before implementing the security recommendations for operating systems described in this chapter, perform all the security steps outlined in your operating system documentation. Security guidelines for operating systems are generally available on vendor Web sites.

Protecting Files and Resources

Protect files and resources in your operating system environment as follows:

- Set up access restrictions to executable files, data files, Web pages, directories, and administrative tools as follows:
  - On each server that is a part of a Siebel deployment, restrict local user access to Siebel directories to Siebel administrators only. This restriction prevents insiders with access to the computer, but without Siebel administrator privileges, from accessing sensitive information that can be used to gain, or elevate Siebel privileges, thereby allowing more significant security violations to occur.
  - For Siebel deployments that store highly sensitive data or that have other high-security requirements, it is recommended that you encrypt the Siebel File System and all server disks containing Siebel Business Applications data, either using third-party products or encryption features provided by your operating system.
  - If you configure Siebel-specific environment variables that include sensitive data on a computer hosting a module in a Siebel deployment, for example, if you have implemented a Siebel Product Configuration Application Object Manager on a dedicated Siebel Server, then encrypting the server disks is also recommended.

    For information on deploying the Siebel Configurator, see *Siebel Deployment Planning Guide*. For information on setting Siebel-specific environment variables, see *Siebel System Administration Guide*.
- Audit file permissions, file ownership, and file access.
- Restrict access to accounts and services.

  Controlling access is an important element in maintaining security. The most secure environments follow the least-privilege principle, which grants users the least amount of access that still enables them to complete their required work. Set up hosts to allow only those services (ports) that are necessary and run only with the fewest possible services. Eliminate services with known vulnerabilities.
- Run the checksum utility on system files when installed and check for Trojan malware frequently. (A Trojan is software that appears legitimate but which contains malicious code that is used to cause damage to your computer.) Check user file systems for vulnerabilities and improper access controls.
- Verify operating system accounts and make sure they have passwords that are difficult to guess.
- Automatically disable accounts after several failed login attempts.
- (UNIX) Limit root access.
- Manage user accounts:
  - Do not share user accounts.
  - Remove or disable user accounts upon termination.
  - Require strong passwords.
  - (Windows) Disable automatic logon.
  - (UNIX) Use a restricted shell.

  - (UNIX) Disable login for well-known accounts that do not need direct login access (bin, daemon, sys, uucp, lp, adm).

- Restrict guest accounts:
  - As with any account, create a guest account only for the time required and remove the account when it is no longer required.
  - Use a non-standard account name for the account; avoid the name guest.
  - Use a strong password.
  - (UNIX) Use a restricted shell. If reasonable, give the account an 077 unmask.

Securing the Siebel File System

The Siebel File System consists of a shared directory that is network-accessible to the Siebel Server and contains physical files used by Siebel Business Applications. The Siebel File System stores documents, images, and other types of file attachments.

Requests for access to the Siebel File System by Siebel user accounts are processed by Siebel Servers, which then use the File System Manager (FSM) server component to access the Siebel File System. FSM processes these requests by interacting with the Siebel File System directory. Siebel Remote components also access the Siebel File System directly. Other server components access the Siebel File System through FSM.

A Siebel proprietary algorithm that compresses files in the Siebel File System prevents direct access to files from outside the Siebel application environment in addition to providing a means of encrypting files. This algorithm is used at the Siebel Server level and appends the extension `.saf` to compressed files. These compressed files are decompressed before users or applications access them. Users access decompressed files through the Web client. You cannot disable use of this algorithm. For more information about the Siebel File System, see *Siebel System Administration Guide*.

To provide additional security for the Siebel File System, implement the following recommendations:

- When creating the shared directory for the Siebel File System, append a dollar sign ($) to the end of the share name; this hides the shared directory on the network. For example:

  ```
  \\servername\siebelfs$
  ```

- Use third-party utilities to encrypt the file system or individual folders within the file system.
- Make sure that the Siebel application does not provide direct user access to the Siebel File System by restricting access rights to the Siebel File System directory to the Siebel service owner and the administrator. For information, see "Assigning Rights to the Siebel File System" on page 4-3.
- Restrict the types of files that can be saved in the Siebel File System as described in "Excluding Unsafe File Types from the Siebel File System" on page 4-5.

Assigning Rights to the Siebel File System

This topic describes how to restrict access rights to the Siebel File System directory to the Siebel service owner and the administrator.

The processes and components of the Siebel Server use the Siebel service owner account to operate. Do not give the Siebel service owner account permission to access any directory other than the Siebel File System directory and the Siebel Server directories.

> **Note:** If Active Directory authentication is implemented, then all users require read, execute and modify permissions to the Siebel File System `\userpref` directory to save their user preferences. In this case, when assigning rights to the Siebel File System, you must assign read, execute and modify permissions to the overall Siebel File System directory to everyone, assign read, execute and modify permissions to the `\userpref` directory to everyone, then restrict access to all other directories in the Siebel File System to the administrator and the Siebel service owner.

The following procedures describe how to assign rights to the Siebel File System on Windows and UNIX platforms.

Assigning Rights to the Siebel File System on Windows

Use the following procedure to assign the appropriate rights to the Siebel File System on Windows.

To assign the appropriate rights to the Siebel File System on Windows

1. In Windows Explorer, navigate to the Siebel CRM directory, for example, SBA_82.
2. Right-click the Siebel CRM directory, and select the Sharing and Security option.
3. Click the Security tab.
4. Select the Advanced option.
5. Deselect the Inherit from parent permissions check box.
6. When prompted, select the Remove option.
7. Check the Replace permission entries on all child objects option.
8. Click Add and assign full control permissions to administrators and the Siebel Service account. Administrators require full rights on the Siebel File System to perform backup or recovery tasks

   > **Note:** If Active Directory authentication is implemented in your environment, then assign read, execute, and modify permissions to all other users.

9. Click OK.

   The file permissions are replicated on all child objects.

10. (Active Directory Only) In an Active Directory authentication environment, for each directory in the Siebel File System except the `\userpref` directory, remove all permissions for user accounts, except for the administrator and the Siebel Service user accounts.
11. Repeat this procedure for the Document Server directory. Assign file system rights through the Microsoft Management Console and the security template snap-in.

Assigning Rights to the Siebel File System on UNIX

Use the following procedure to assign the appropriate rights to the Siebel File System on UNIX.

To assign the appropriate rights to the Siebel File System on UNIX

1. Log in as root to the file system server.
2. Using the appropriate administrative tools for your UNIX operating system, verify that only the Siebel Service account and the Siebel administrator have read, write, and execute permissions to the Siebel File System directory; remove permissions to the Siebel File System directory for all other users.

   For example, run the following command to remove all permissions (read, write, and execute) to the Siebel File System directory for all users and groups except the owner of the Siebel File System directory (Siebel Service account):

   ```
   chmod -R go-rwx FileSystemDirectory
   ```

   where *FileSystemDirectory* is the name of the Siebel File System directory.

Excluding Unsafe File Types from the Siebel File System

You can prevent files with a specific file extension from being saved to the Siebel File System by enabling the File Ext Check system preference. This topic describes how to implement file extension checking, and how to specify the file types you want to exclude from the Siebel File System.

When you select a file type to be excluded, Siebel Application Object Manager components are prevented from adding any files with that file extension to the Siebel File System, including files from external sources, such as Siebel CRM Desktop, or files from a custom integration point which the Enterprise Application Integration (EAI) Application Object Manager might attempt to add.

> **Note:** Files with file extensions that you choose to exclude that are added to the Siebel File System before you implement file extension checking are not removed from the system. You must review and remove these existing files manually, if required.

About Potentially Unsafe File Types

The purpose of excluding files with specific file extensions from the Siebel File System is to protect your Siebel CRM implementation from viruses or other malicious code potentially contained in these files. Executable files, such as batch files and program execution files, which are designed to run tasks automatically, are the most obvious types of files you might want to exclude. Table 4–1 provides a brief list of executable files on Windows and UNIX.

Table 4–1 Executable Files

Extension	Operating System
bat	Windows
bin	Windows and UNIX
cmd	Windows
com	Windows

Table 4–1 (Cont.) Executable Files

Extension	Operating System
csh	UNIX
exe	Windows
inf	Windows
jse	Windows
ksh	UNIX
reg	Windows
run	UNIX
sh	UNIX
vbe	Windows
vbs	Windows

For additional information on unsafe file types, see the following:

- The Microsoft Support Web site provides information about unsafe file extensions, and it lists the files included in the Unsafe File List used in Internet Explorer. Go to

  `http://support.microsoft.com/kb/925330`

- The WinZip Computing Web site provides information on unsafe file types, and it lists the file extensions that WinZip treats as unsafe. Go to

  `http://kb.winzip.com/help/winzip/ZipSecurity.htm`

Enabling File Extension Checking

Perform the steps in the following procedure to enable file extension checking.

To enable file extension checking

1. Log in to a Siebel application on the Siebel Server.
2. Navigate to Administration - Application, and then the System Preferences view.
3. In the System Preferences list, either query for the system preferences shown in the following table, or create the system preferences if they do not already exist, then enter values similar to those shown.

Table 4–2 System Preferences List

System Preference Name	System Preference Value
DCK:Flag For File Ext Check	Enter either Y or N to indicate whether or not you want to enable file extension checking. The default value is N.
DCK:Excluded File Ext	Enter the file extensions you want to exclude in the following format: `file extension1,file extension2,file extension`*n* For example: `bat,bin,cmd,com,csh,exe,txt,gif,jpg` You can enter up to 100 characters in the System Preference Value field. If you want to specify additional file extensions to exclude, then create one or more DCK:Excluded File Ext *N* system preference entries.

Table 4–2 (Cont.) System Preferences List

System Preference Name	System Preference Value
DCK:Excluded File Ext *N*	If you want to exclude file extensions that cannot be accommodated in the DCK:Excluded File Ext system preference, then use this system preference to specify the additional file extensions. ■ In the System Preference Name field, change the value of *N* to a number between 1 and 9, starting with 1 and increasing incrementally up to 9 with each additional DCK:Excluded File Ext *N* entry you create. ■ In the System Preference Value field, enter the additional file extensions you want to exclude in the following format: `file extension1,file extension2,file extension`*`n`* You can enter up to 100 characters in the System Preference Value field. **Note** that if the DCK:Excluded File Ext system preference does not exist, the DCK:Excluded File Ext *N* system preference is not processed.

4. Stop then restart the Siebel Server for the new system preference values to take effect.

About File Extension Checking on the Siebel Mobile Web Client

You can configure file extension checking on the Siebel Server and on Siebel Mobile Web Clients. To implement new system preference values defined on the Siebel Server on the Siebel Mobile Web Client, synchronize the Siebel Mobile Web Client with the Siebel Server, then stop and restart the Siebel Mobile Web Client.

The file extension checking settings you specify at the Siebel Server level take precedence over Siebel Mobile Web Client settings. For example, if the file extension .exe is among the list of excluded file extensions on the Siebel Server, but is not excluded by the Siebel Mobile Web Client, when the Siebel Web Client connects to the Siebel Server to synchronize the local database, the following occurs:

- All attachment records with the .exe file extension are rejected for synchronization with the enterprise database
- A delete operation for each attachment record of type .exe is generated

During the next synchronization session, the delete operations for the rejected attachment records are executed on the Siebel Mobile Web Client and all the attachment records with the extension .exe are deleted.

Assigning Rights to the Siebel Service Owner Account

Siebel Business Applications are installed using the Siebel service owner account. This account must belong to the Windows domain of the Siebel Enterprise Server (Windows environments) or to the users group of the Siebel Enterprise Server (UNIX environments) and must have full write permissions to the Siebel File System.

Implement the following recommendations for the Siebel service owner account:

- Make sure a strong password has been set for the Siebel service owner account.

  For information on changing the password for the Siebel service owner account, see *Siebel Security Guide*.

- Set the user account policy to lock the account after three unsuccessful login attempts.

- Assign appropriate rights for the account as described in the following procedures.

For information on creating the Siebel service owner accounts, see *Siebel Installation Guide* for the operating system you are using.

Assigning Rights to the Siebel Service Owner Account on Windows

The following procedure describes how to assign rights for the Siebel service owner account on Windows.

To assign appropriate rights to the Siebel service owner account on Windows

1. From the Start menu, select Settings, Control Panel, Administrative Tools, and then choose Local Security Policy.
2. Select Local Policies.
3. Click User Rights Assignments.
4. Assign the following rights to the Siebel service owner account:
   - Act as part of the operating system
   - Lock pages in memory
   - Bypass traverse checking
   - Log on as a service
   - Replace a process level token
   - Deny logon locally

   Do not assign Siebel service owner accounts any rights other than those listed. Siebel Service accounts must belong only to the Local Users Group. Use the local security policy editor to assign user rights for Siebel service owner accounts.

Assigning Rights to the Siebel Service Owner Account on UNIX

The following procedure describes how to assign rights for the Siebel service owner account in a UNIX environment.

To assign appropriate rights for the Siebel service owner account on UNIX

1. Log in as root on the Siebel application server.
2. Using the appropriate administrative tools for your UNIX operating system, for example, the System Management Interface Tool (AIX) or the Admintool (Oracle Solaris), select the user who runs the Siebel service.
3. Check that the Siebel service does not run as the root user.

Note: You must set the execute bit for the `/siebsrvr/webmaster` directory for the Siebel service to function. The Siebel service account requires permission to execute the `netstat` command to perform the installation successfully. Otherwise, the installation fails.

Applying Patches and Updates

Keep track of updates, service packs, hot fixes, and patches. Evaluate the need for patches before installing them on production systems. Test patches on development or staging systems, not on production systems, because security patches can disable services or introduce additional vulnerabilities. Set up a process for testing and implementing any updates for Siebel CRM that are released. See the Oracle Critical Patch Updates and Security Alerts Web site at

http://www.oracle.com/technetwork/topics/security/alerts-086861.html

5

Securing the Siebel Database

This chapter outlines recommendations for securing your Siebel database after you have performed the security procedures prescribed by your database vendor. For information on these procedures, refer to your relational database management system documentation. This chapter includes the following topics:

Restricting Access to the Siebel Database

Sensitive user information, such as credit card numbers, customer details, email IDs, and so on, is usually stored in the database that an application is using. It is important to classify the data that is stored in the database and to implement a role-based access system.

Define stringent policies for Siebel database access both at the account-login level and at the network-visibility level. Only assign authorized users, for example, approved database administrators (DBAs), system accounts for root usage and remote access to the server.

Define access rules so that users cannot log in to the Siebel database and execute queries. Follow these guidelines for the operating systems:

- **Windows.** Add all general users to the Public group in the Siebel database and assign appropriate rights.
- **UNIX.** Do not grant database administrator privileges to general users.

For additional information, see your RDBMS documentation.

Reviewing Authorization Policies

Implement the following recommendations:

- Restrict access to SQL trace and log files.

  In a production environment, do not run Siebel Business Applications with a high level of logging, for example, use log level 2, not 5.

- Restrict remote access to the operating system, such as through Telnet (Terminal Network), and restrict remote access diagnostics programs.

- Limit access to the data dictionary files; these files store metadata about schema definitions, visibility rules, and other items.

Protecting Sensitive Data in the Siebel Database

It is recommended that you protect sensitive application data in the Siebel database by encrypting the data. You can choose to encrypt the following:

- Specific database fields
- Specific database tables
- The entire database

Siebel Business Applications support field-level encryption of sensitive information stored in the Siebel database, for example, credit card numbers or national identity numbers. You can configure Siebel Business Applications to encrypt field data before it is written to the Siebel database and decrypt the same data when it is retrieved. This configuration prevents attempts to view sensitive data directly from the Siebel database.

Siebel Business Applications support data encryption using Advanced Encryption Standard (AES). By default, data encryption is not configured. It is recommended that you set data encryption for business component fields using Siebel Tools. For information on encrypting data, see *Siebel Security Guide*.

When field-level encryption is implemented, data is not decrypted until it is displayed by a user who has the necessary privileges to view the data. The data remains encrypted even when it is loaded into memory, which increases data security. However, using field-level encryption affects performance.

As an alternative to field-level encryption, you can secure sensitive data using products such as the following:

- **Transparent Data Encryption.** If you are using a Microsoft or Oracle database with Siebel Business Applications, then you can use the Transparent Data Encryption feature to encrypt data in the Siebel database. Oracle databases support the use of Transparent Data Encryption to encrypt data at the column and tablespace level. Microsoft databases support the use of Transparent Data Encryption to encrypt data at the cell and database level.

  Transparent Data Encryption encrypts data when it is written to the database and decrypts it when it is accessed by Siebel Business Applications. Application pages are decrypted as they are read and are stored in memory in clear text. Because the data is not encrypted when it is being sent to Siebel Business Applications, you must also enable TLS to protect communications between the server and clients. The performance impact of implementing Transparent Data Encryption is minimal.

  If you enable Transparent Data Encryption, then all database file backups are also encrypted. For information about Oracle support for Transparent Data Encryption, go to the Oracle Technology Network Web site at

  http://www.oracle.com/technetwork/database/options/advanced-security/index-099011.html

  For information about Microsoft support for Transparent Data Encryption, go to the Microsoft MSDN Web site at

  http://msdn.microsoft.com/

- **Oracle Database Vault.** If you are using an Oracle database with Siebel Business Applications, then you can use Oracle Database Vault to restrict access to all the schemas and objects in your application database, or to individual objects and schemas by users, including users with administrative access to the database.

  Oracle Database Vault allows you to define a Realm, a protection boundary, around all or some of the objects in your database. The database administrator can work with all the objects within the Realm but cannot access the application data that they contain. This restriction protects your data from insider threats from users with extensive database privileges.

  You can integrate Oracle Database Vault with Transparent Data Encryption without the need for additional configuration. For additional information on Oracle Database Vault, go to the Oracle Technology Network Web site at

  `http://www.oracle.com/technetwork/database/options/database-vault/index-085211.html`

Maintaining Database Backups

Implement the following database backup policies:

- Back up the Siebel database at regular intervals and store the backups securely for the period required by your organization’s retention policies.
- Limit access to the backups to authorized users.
- Encrypt Siebel database backups.
- Secure the devices on which the Siebel database backups are stored.

6

Securing Siebel Business Applications

This chapter describes how to protect Siebel Business Applications by configuring the security features. This chapter includes the following topics:

About Securing Applications

Securing applications requires analysis, monitoring, and testing. Protecting applications is crucial because an attacker who has taken over an application can execute commands with the privileges of that application. Often application-to-application security is minimal and privileges are high because these are assumed to be trusted sources. Many applications run with superuser (root) privileges, which increases the risk of serious damage if a vulnerability is exploited.

Web applications are the leading entry for most hackers and have more vulnerabilities than other applications. Web server and application server configurations play a key role in the security of a Web application. These servers are responsible for serving content and calling applications that generate content. In addition, many application servers provide several services that Web applications can use including data storage, directory services, email, messaging, and so on.

Several server-configuration problems can threaten a Web site, for example:

- Server-software configurations that permit directory listing and directory traversal attacks
- Unnecessary default, backup, or sample files including scripts, applications, configuration files and Web pages
- Improper file and directory permissions

- Unnecessary services enabled, including content management and remote administration
- Default accounts and passwords
- Administrative or debugging functions that are enabled or accessible
- Poorly configured TSL certificates and encryption settings
- Use of self-signed certificates to achieve authentication
- Use of default certificates

You can detect many of these problems with security-scanning tools. These configuration problems can compromise a Web application and successful attacks can also result in the compromise of back-end applications, including databases and corporate networks.

A strong Web application is typically deployed on a secure host (server) in a secure network using secure design and deployment guidelines. Because of the dependencies on the network environment, Web application security must be addressed in multiple layers, including securing the network, host, and application.

Guidelines for Deploying Siebel Business Applications

This topic provides guidelines for minimizing security vulnerabilities when deploying Siebel Business Applications. Consider the following:

- **Verify that the environment in which Siebel Business Applications is to be deployed is secure.** Verify that the underlying platform (operating system, Web server, and database server) upon which Siebel Business Applications reside or are connected to has been secured using the respective vendor's security guides and has been checked against your organization's security policy.
- **Do not configure an email relay service or other communications service on any of the computers where Siebel Business Applications reside.** If email is needed, then permit only outgoing email to notify administrators of any critical events. With applications such as Siebel Email Marketing, configure the Siebel Server to forward the emails to an email relay service on another server in the demilitarized zone, which can forward the emails to the appropriate destination. For additional information, see *Siebel Marketing Installation and Administration Guide*.
- **Enforce a server-management policy.** For example, system administrators log in to servers using their respective personal user IDs and password (with administrative privileges) instead of the default administrator accounts.
- **Delete optional learning aids. For example, delete the sample Siebel database and demo data.** For information on deleting the sample Siebel database, see *Siebel Installation Guide* for the operating system you are using.
- **Disable or uninstall optional Siebel Business Applications components that are not required in your environment.** For information, see "About Disabling Siebel Components" on page 6-3.
- **Install application-specific patches.** For additional information on the patches available with Siebel Business Applications, see "Critical Patch Updates for Siebel Business Applications" on page 2-3.
- **Store all application-specific files in a directory.** Limit the attack surface to this directory and any subdirectories it contains.
- **Add application-layer authentication.**

About Disabling Siebel Components

Most of the components required to run Siebel Business Applications are common to all Siebel Business Applications. However, the components that are required in a specific Siebel environment vary according to factors such as the following:

- Whether the Siebel application runs in high-interactivity or standard-interactivity mode
- Whether mobile clients are supported
- The features provided by the Siebel application, for example, Siebel Sales uses a number of components that are not required by applications such as Oracle's Siebel Marketing or Oracle's Siebel Employee Relationship Management application

During the Siebel Server configuration process, you specify the components and component groups you want to enable for a Siebel Server. It is not necessary to run all components on all Siebel Servers in an Enterprise. Verify that only the components or component groups you require on each Siebel Server are enabled; disable or unassign component groups that are not required.

The following are some examples of Siebel Server components that do not have to be enabled on all Siebel Servers in an Enterprise:

- **SvrTblCleanup.** The SvrTblCleanup component deletes completed and expired Server Request records for all Siebel Servers in a Siebel Enterprise from the S_ SRM_REQUEST table. Enable this component on only one Siebel Server in a Siebel Enterprise.
- **SCBroker**. Disable the SCBroker component on Siebel Servers that host only batch mode components, for example, Workflow components.
- **SRProc.** Disable the Server Request Processor (alias SRProc) component on Siebel Servers that run only Application Object Manager components and that do not run batch mode components.

Components can be disabled using the Siebel Administration - Server screens or the srvrmgr command-line interface. For information on enabling and disabling components, see *Siebel System Administration Guide*.

About User Authentication

Siebel Business Applications have an open authentication architecture that integrates with your selected authentication infrastructure. Siebel Business Applications support these types of user authentication:

- A database security adapter for database authentication
- An LDAP or ADSI security adapter for LDAP or Active Directory authentication
- Web Single Sign-On (SSO)
- Custom security adapter

  You can develop a custom security adapter using a security adapter SDK, which allows you to implement authentication using products such as RACF, CA-ACF2 or CA-TopSecret.

It is recommended that you implement LDAP or Active Directory authentication or Web SSO authentication. It is simpler to maintain these methods of authentication and to apply account policies to them. For a comparison of the benefits and disadvantages of the supported authentication mechanisms, see the chapter on security adapter authentication in *Siebel Security Guide*.

Implementing Password Management Policies

It is important to implement a password management policy so that only authorized users can access Siebel Business Applications. The details of the policy are likely to vary across Siebel implementations, depending on the language and character set in use in a Siebel environment, and depending on the business needs of users. However, a set of rules need to be defined, implemented, and checked each time a new password is created or modified.

Implement the password management recommendations in the following topics:

- "General Password Policies" on page 6-4
- "Defining Rules for Password Syntax" on page 6-5
- "About Configuring Password Hashing for Users" on page 6-5

General Password Policies

Implement the following general password management policies:

- Determine a password expiry period (except for the Siebel administrator).
- Determine the number of password failures allowed before an account is locked.
- Implement password syntax rules. See "Defining Rules for Password Syntax" on page 6-5.
- Implement password hashing. For additional information, see "About Configuring Password Hashing for Users" on page 6-5.
- Change the password of the SADMIN account regularly.

  During the Siebel Business Applications installation process, the Siebel administrator account (SADMIN) is created. You are required to specify a password for this account before you install and configure the Siebel database components. Change the password for the administrator account at regular intervals. For information on this task, see *Siebel Security Guide*.
- Change the password for Siebel utilities after installation.

A number of Siebel command-line utilities can be used during the installation and configuration of Siebel Business Applications, for example:

- **srvrmgr**
- **srvrcfg**
- **srvredit**

When starting any of these utilities, you must specify the Siebel administrator user name and password in the command line as command flags. In a Siebel deployment with high-security requirements, it is recommended that you change the Siebel administrator user name and password used for these utilities after you have completed the Siebel implementation process.

Defining Rules for Password Syntax

To make sure that the passwords in your Siebel deployment are difficult to guess and are capable of withstanding brute-force attacks, define rules for your organization relating to password syntax. It is recommended that you implement password syntax rules similar to the following:

- The password value must not be the same as the user name.
- Password values must include a variety of characters within the supported character set, for example:
  - Both alphabetic and numeric characters are required.
  - A special character is required, such as a symbol, an accented character, or a punctuation mark.
  - At least one uppercase and one lowercase letter is required.
  - Specify illegal values, for example, no more than one space character is permitted, or no more than 2 repetitions of the same character are permitted.
- Password values must be a minimum length, usually 8 characters.

In general, Siebel Business Applications do not provide support for either implementing password syntax rules or for verifying them. However, the following options exist:

- For the Siebel Mobile Web Client, the following options for managing the passwords of Remote clients are available:
  - Application lockout after a specified number of consecutive, unsuccessful login attempts
  - Password expiration after a defined interval
  - Password syntax check
  - User password reset by the administrator

  For information on setting these options, see *Siebel Remote and Replication Manager Administration Guide*.
- Users who have previously self-registered on a Siebel customer or partner application who forget their passwords can get new passwords by clicking the Forgot Your Password? link in the login dialog box. You can configure the length (maximum and minimum characters) of the passwords generated by your Siebel application for such users. For additional information, see *Siebel Security Guide*.

About Configuring Password Hashing for Users

Password hashing is a critical tool for preventing unauthorized users from bypassing Siebel Business Applications and logging in to the Siebel database directly. It also prevents passwords intercepted over the network from being used to access Siebel Business Applications, because an intercepted hashed password is itself hashed when a login is attempted, leading to a failed login.

Password hashing is not enabled by default in Siebel CRM. It is recommended that you enable password hashing after installing Siebel Business Applications if appropriate for your environment.

Password hashing is enabled by setting the value of the HashUserPwd parameter to True and hashing each user password using the hashpwd.exe utility. For detailed information on enabling password hashing, see *Siebel Security Guide*.

Reviewing Special User Privileges

Within Siebel Business Applications, special users are defined with specific roles within the application. Data to support these special user accounts is included in the seed data installed with Siebel Business Applications. You can change special user account names after installation, or delete the relevant seed data for a special user account if you do not need the functionality it provides. Do not, however, disable the SADMIN or guest user accounts.

The following special users are defined:

- **Anonymous users.** You can define an anonymous user (or guest) account to allow access to your Siebel application by unregistered, unauthenticated users. You must also define an anonymous user if your Siebel application implements LDAP or Active Directory authentication.

  Three Siebel application user accounts, GUESTCST, GUESTCP, and GUESTERM are provided as seed data for use as anonymous user accounts; however, you can create a different user account for this purpose. Review the user responsibilities assigned to the anonymous user record and limit them to those necessary for sign-on and guest access.

  Anonymous browsing is enabled by default. If your Siebel application does not use functionality that requires anonymous browsing, then set the AllowAnonUsers parameter to False. For further information, see *Siebel Security Guide*.

- **Administrator users.** A Siebel administrator database account (default user ID is SADMIN) and a Siebel application user account, SADMIN, are created during the Siebel Business Applications installation process for the administrative user. Follow these guidelines in relation to the administrator user:

  – Limit usage of the administrator role.

    Review users with administrative responsibilities. In Siebel Business Applications, the SADMIN responsibility has broad administrative privileges. For this reason, regularly review the list of users with this responsibility. Define and assign appropriate responsibilities for users that clearly reflect their line of duty.

  – Delete or disable unused administrator user IDs.

- **Directory application user.** The Directory Application User is a special user defined to handle access to the LDAP directory and to Active Directory if these authentication mechanisms are used. By setting up an application user as the only user with search, read, and update privileges to the directory, you minimize the level of access of all other users to the directory.

  The directory application user must not have a corresponding database account and must not be defined as a Siebel application user or have a Siebel application user record.

- **Shared database account user.** If you are using LDAP, Active Directory, or Web SSO authentication, then you can configure a shared database account in the directory; this is a directory entry that contains a database account that is shared by many users. A database login is created for all Siebel users who are authenticated externally during the installation process; the default database login is LDAPUSER. You must also specify a valid Siebel user ID and password for the shared database account in the directory.

- An employee record, Proxy Employee, is provided as seed data during installation. This record provides customers (contact users) who log in to a Siebel customer application with a user ID (PROXYE), a position (Proxy Employee), and an organization (Default Organization).

  Because the PROXYE user ID gives view access to data that is associated with the related organization, review the visibility to data provided by the proxy employee user ID and, if necessary, change the organization with which the Proxy Employee user record is associated. You cannot change seed data, therefore, to modify the Proxy Employee record you must make a copy of the record, rename it, and amend the copy. For additional information, see *Siebel Security Guide*.

About Implementing Authorization and Access Control

This topic describes the mechanisms that you can use to restrict access to data and Siebel Business Applications functionality for authenticated users after they have accessed Siebel Business Applications.

Siebel Business Applications use two primary access-control mechanisms to determine the privileges or resources that a user is entitled to within Siebel Business Applications:

- **View-level access control.** Manages the functions that a user can access.
- **Record-level access control.** Manages the data items that are visible to each user.

View-Level Access Control

Organizations are generally arranged around functions, with employees being assigned one or more functions. View-level access control determines what parts of a Siebel application a user can access. This access is based on the functions assigned to that user. In Siebel Business Applications, these functions are called *responsibilities*. Responsibilities define the collection of views to which a user has access. Each user's primary responsibility also controls the user's default screen tab layout and tasks.

You can choose to store users’ Siebel responsibilities as roles in a directory attribute instead of in the Siebel database if you are using LDAP, ADSI, or custom security adapters, or if you are using Web SSO authentication.

Record-Level Access Control

Record-level access control assigns permissions to individual data items within an application. This access level allows you to configure a Siebel application so that only authenticated users who need to view particular data records can access that information.

Siebel Business Applications use three types of record-level access: position, organization, and access group. When a particular position, organization, or access group is assigned to a data record, only employees within that position, organization, or access group can view that record.

Adhere to the following general guidelines when authorizing access to views and records:

- Grant privileges to positions and responsibilities rather than to individual named users, and grant necessary privileges only.
- Limit access to the user profiles and position lists.

  For additional information, see "Implementing Personal Visibility for the User Profile View" on page 6-8.

- Lock accounts after invalid login attempts.

For additional information on view and data access control, see *Siebel Security Guide*.

Implementing Personal Visibility for the User Profile View

This topic outlines how to strengthen the security of the User Profile View by enforcing personal access control to the view. This ensures that access to the data in the view is restricted to the user whose person record is associated with the data in the database. To enforce personal access to a view, you must set the Visibility Type of the view to Personal. This task is described in the following procedure.

> **Note:** It is recommended that you set the Visibility Type to Personal for all View applets that contain sensitive information.

To implement personal visibility to the User Profile View

1. Start Siebel Tools.
2. In the Object Explorer, click the View object type.

   The Views list appears.
3. Query for the User Profile Default View view.
4. Confirm that the property settings are set as follows:
   - **Visibility Applet.** Set to User Profile Form Applet.
   - **Visibility Applet Type.** Set to Personal.
5. In the Object Explorer, expand the View object type, select View Web Template, expand the View Web Template object type, and then select the View Web Template Item object type.
6. In the Object List Editor, select the User Profile Form Applet object.
7. Lock the object, then change the property setting to the following:

   Applet Visibility Type. Set to Personal.
8. Navigate to Business Component in the Object Explorer.
9. Query for Employee.
10. Lock the object.
11. In the Object Explorer, expand the Business Component object, then select the BusComp View Mode object.
12. Create a new record with the following property values.

Field	Value
Name	Personal
Owner Type	Person
Visibility Field	Row Id

13. Compile the SRF.

For additional information on configuring access control, see *Siebel Security Guide*.

About Securing Application Data During Configuration

This topic outlines recommendations for securing Siebel Business Applications data when performing configuration tasks. In addition to applying critical patch updates, encoding relevant data, and implementing secure coding practices, perform the recommendations in the following topics:

- "About Using Web Services" on page 6-9
- "About Defending Data from HTML Injection" on page 6-9
- "About Using External Business Components" on page 6-11
- "About Using HTTP Methods" on page 6-11

About Using Web Services

When creating, implementing, and publishing Web services, implement the WS-Security UserName Token mechanism to pass user credentials (Username and Password) to Web services. Passing the user name and password in the Web service URL is not supported in Siebel CRM version 8.1 or 8.2.

Using the WS-Security UserName Token mechanism means that user names and passwords do not have to be passed to Web services in the URL and a session cookie does not have to be passed with the HTTP request. For additional information on the WS-Security UserName Token, see *Integration Platform Technologies: Siebel Enterprise Application Integration*.

When you create an inbound Web service based on a Siebel business service or a Siebel workflow process, make sure that the Web service is secure. Siebel CRM does not verify the security of inbound Web services you create.

About Defending Data from HTML Injection

This topic describes measures you can take to protect Siebel application data from HTML injection attacks.

Displaying HTML Content

Siebel Business Applications allow you to display HTML content in fields in the user interface. When using Control objects that are field values, you can set the value of the HTML Display Mode property to control how the field value is displayed in the user interface. You can specify the following values for the HTML Display Mode property:

- **EncodeData.** If the field value contains HTML reserved characters, then they are encoded before they are displayed so that the HTML displays as text in the user interface and is not executed as an HTML command. It is recommended that you set the HTML Display Mode property to EncodeData for each Control object to ensure executable statements are not included in Siebel data records.
- **DontEncodeData.** Use this value only when the value of the field is HTML text and you want the HTML to be executed. Selecting this value is not recommended because the HTML text can be the object of malicious interference.
- **FormatData.** This value is used when description or comment fields are in read-only layout. Setting FormatData to TRUE causes data to be formatted in HTML. For further information, see *Siebel Object Types Reference*.

Oracle recommends that you review all Control objects whose HTML Display Mode property is set to either DontEncodeData or FormatData, and consider changing the value of the property to EncodeData. The following SQL commands can be used to return a list of Control objects that have the HTML Display Mode property set to a value of either FormatData or DontEncodeData:

```
SELECT
      HTML_DISPLAY_MODE
FROM
      SIEBEL.S_CONTROL
WHERE
      HTML_DISPLAY_MODE = 'FormatData' OR
      HTML_DISPLAY_MODE = 'DontEncodeData'
```

Review the list of Control objects returned in the query. You cannot change the value of the HTML Display Mode property to EncodeData for all Control objects in one operation from within the Siebel application. The property must be set for each control individually.

If you choose another method of changing the HTML Display Mode property to EncodeData for all the Control objects returned in the query, then consider the consequences carefully before proceeding. It is recommended that you contact your Oracle sales representative for Oracle Advanced Customer Services to request assistance with this task.

Specifying Trusted Server Names

To strengthen your Siebel application and data against attacks, you can specify the name of each of the host servers that are authorized for use with the Siebel application. The following procedure describes how to specify the names of these trusted servers.

To specify the names of trusted servers

1. Start Siebel Tools.
2. In the Object Explorer, select the Application object type.

   The Applications list appears.
3. Query for the name of your Siebel application in the Object List Editor.

   For example, for the Siebel Call Center application, query for Siebel Universal Agent.
4. Lock the application object.
5. In the Object Explorer, expand the Application object type, then select the Application User Prop object type.

   The Application User Props list appears.
6. In the Object List Editor, add an application user property for each server used by the Siebel application. For example:

   ```
   Name: AllowedServerNamesUrl0 value:server_name1
   Name: AllowedServerNamesUrl1 value:server_name2
   ```
7. Compile the project associated with the application into an SRF file.

About Using External Business Components

External business components are used to access data that resides in a non-Siebel table or view using a Siebel business component. When configuring external business components, you must specify the data source for the external table that contains the data you want to access.

To prevent users having to log in when accessing the external data source, for each data source accessed by an external business component, specify the data source user name and password details using the DSUsername and DSPassword values when configuring the data source named subsystem. The DSUsername and the DSPassword parameters are activated only when using the database security adapter. For information on configuring external business components, see *Integration Platform Technologies: Siebel Enterprise Application Integration*.

About Using HTTP Methods

The HTTP protocol supports a number of methods that are used to specify the operation to be performed on a resource on the Web. Siebel Business Applications support the HTTP GET and POST methods only. All other HTTP methods are blocked to maximize the security of your Siebel application. For information on using the HTTP GET and POST methods with Siebel Business Applications, see *Transports and Interfaces: Siebel Enterprise Application Integration*.

In Siebel Innovation Pack 2014 and later, you can allow access to a blocked method for HTTP GET access using the GETEnabledMethods user property. For information about using the GETEnabledMethods user property, see *Configuring Siebel Open UI*.

About Message Broadcasting

Siebel message broadcasting functionality allows Siebel administrators to display important information directly in the message bar of users' screens. The text of a message broadcast can be up to 2,000 characters in length and can contain HTML tags, which are treated as HTML code on the message bar.

Message broadcasting is available for employee applications but not for customer or partner applications. By default, message broadcasting is enabled, although the administrator can enable or disable it. In environments with very high security requirements, it is recommended that message broadcasting be disabled. For information on disabling message broadcasting, see *Siebel Applications Administration Guide*.

About Securing Third-Party Applications

Secure third-party applications by making sure that all the software is updated with the latest software versions and security patches. For additional information on securing third party products, see the vendor-specific documentation.

7

Implementing Auditing

This chapter contains recommendations for implementing auditing in a Siebel Business Applications deployment so that suspicious activities are detected. This chapter contains the following topics:

- Operating System Auditing
- Database Auditing
- Siebel Business Applications Event Logging
- About Siebel Audit Trail

Operating System Auditing

Implement the following operating system auditing recommendations:

- Use platform-level auditing to audit login and logout events, access to the file system, and failed object access attempts.
- Back up log files and regularly analyze them for signs of suspicious activity.
- Secure log files by using restricted access control lists, and relocate system log files away from their default locations to make sure attackers cannot cover their tracks.

For additional information on operating system auditing, see your operating system documentation.

Database Auditing

Implement the following database auditing recommendations:

- Enable Siebel Audit Trail to audit access to specific data fields or objects in the Siebel database. Enabling Siebel Audit Trail produces a log file of all the events that have occurred, which allows the Siebel database administrator to review the events and detect any suspicious activities. For further information, see "About Siebel Audit Trail" on page 7-2.
- You can also implement database auditing that is included with all supported databases. All vendors support high levels of audits: B3 or C2 Orange book levels. Database auditing requires a security person to review the audit information.

For information on configuring database auditing, see your database vendor documentation.

Siebel Business Applications Event Logging

Configure event logging for the Siebel Server and server components to monitor the internal operation of Siebel Business Applications. You can specify the type and extent of the information logged for a specific Siebel Server or component event by choosing a log level for the event, for example, you can choose to only log error messages or to log detailed information relating to an event.

Table 7–1 shows Siebel Server and component event log levels. The log level determines the amount of information that is written to the log file and the severity of the event logged. For example, if you set the log level to a low number, then only information relating to the most severe events is logged. If you set the log level to a high number, then less severe events are also logged and more information is written to the log for each event.

Table 7–1 Event Log Levels

Event Log Level	Description
0	Fatal events are logged.
1	Error messages and fatal events are logged.
2	Warning messages are logged in addition to error messages and fatal events.
3	Informational messages are written to the log files in addition to all the messages logged for log levels 0-2.
4	Detailed information is written to the log files for all items logged for log levels 1-3.
5	Diagnostic information is written to the log files as well as all the information logged for log levels 1-4.

Implement the following recommendations when configuring event logging:

- Verify that Siebel Business Applications do not log excessive or sensitive information by default, for example, session IDs.
- In a production environment, do not set event log levels for Siebel Server components to verbose levels; the recommended log levels are 2 (Warnings) or 3 (Informational). Do not log sensitive information at the maximum logging settings.

Event logging is configured using the Siebel Administration - Server Configuration screens or the srvrmgr command-line interface. For detailed information on setting event logging for Siebel Server and server component events, see *Siebel System Monitoring and Diagnostics Guide*.

About Siebel Audit Trail

Siebel Audit Trail creates a history of the changes that have been made to data in Siebel Business Applications. Audit Trail functionality is enabled in Siebel Business Applications by default.

Siebel Business Applications support various degrees of auditing:

- At the simplest level, each data record contains the following fields, which store the date and time of each change made to the record, and values identifying the user who made the change:
  - CREATED

  - CREATED_BY
  - LAST_UPD
  - LAST_UPD_BY

  With additional configuration, you can generate an activity for additional levels of auditing. This configuration is best used when there are limited needs for auditing, for example, just a few areas to track.

  > **Note:** If Siebel Enterprise Application Integration (EAI) implements anonymous logins, then Siebel Audit Trail cannot relate a change to the specific user who made the change.

- Siebel Business Applications can maintain an audit trail of information that tells when business component fields have been changed, who made the change, and the value of the field before and after the change. It is also possible to maintain an audit trail of when the business component fields have been viewed or exported and who viewed or exported the fields.

  You can also configure Siebel Audit Trail to determine the scope of the audit. You can choose to audit all activity, or to limit the scope of auditing to those operations performed by certain responsibilities, positions, or employees.

- Using Siebel Workflow, you can configure workflow processes to save information on changes to specific business components.
- You can also attach scripts to the business component Write_Record event and save information about the transaction.

  > **Note:** Be aware that enabling high levels of auditing, for example, log level 5, can have an adverse impact on performance.

Restrict access to the audit records, and archive and delete audit records regularly. For information on configuring and using Siebel Audit Trail, see *Siebel Applications Administration Guide*.

8

Performing Security Testing

This chapter describes how to test the security of your Siebel Business Applications deployment. It includes the following topics:

- About Performing Security Assessments
- About the Common Vulnerability Scoring System
- Using Masked Data for Testing

About Performing Security Assessments

Carry out security-risk assessments of your Siebel Business Applications and infrastructure (for example, the operating system and third-party products) periodically to make sure that security policies are being adhered to and to rectify any security vulnerabilities that are identified. In particular, perform extensive security testing of any customizations you make to your Siebel Business Applications before you implement the customizations in a production environment.

It is recommended that you scan your Siebel Business Applications deployment periodically using vulnerability assessment tools to locate security weaknesses. Use a focused approach for risk mitigation rather than focusing on the identification of every possible attack which can be time-consuming. Various tools are available for performing vulnerability assessments:

- Public domain tools, for example, Nessus, Nmap, COMRaider, FileFuzz, and CIS Tools (www.cisecurity.org).
- Other commercially available tools for which an up-to-date vulnerability database is maintained by the vendors. The following tools are generally available for testing system security:
  - WebInspect
  - NTOSpider

About the Common Vulnerability Scoring System

You can use the Common Vulnerability Scoring System (CVSS) to determine the characteristics and severity of a security vulnerability and to assess its impact on your environment. The CVSS is an open, industry-standard method used to score system vulnerabilities.

In the CVSS, vulnerabilities are assessed on three measures: base properties, temporal properties, and environmental properties. The resultant composite score represents the overall risk posed by the vulnerability in your environment. Using the CVSS can help you determine the severity of vulnerabilities that you find and therefore help determine the priority given to resolving them.

The CVSS is maintained by the Forum of Incident Response and Security Teams (FIRST). For additional information on using the CVSS, go to the FIRST Web site at

http://www.first.org/cvss/

A calculator for scoring vulnerabilities using the CVSS method is available from the National Vulnerability Database Web site at

http://nvd.nist.gov/cvss.cfm

Using Masked Data for Testing

If making a copy of the data in your Siebel production database for security testing or development purposes, then mask sensitive data.

Data masking hides sensitive information by replacing it with similar-looking but nonauthentic data. Effective methods of data masking protect the original data by ensuring it cannot be recovered from the masked data while providing a version of the data that is functionally equivalent for testing purposes. Data, such as personal details and credit card information, must always be masked when used outside the production environment.

Siebel Business Applications do not provide data masking features; this functionality is provided by the RDBMS vendor. The Oracle Data Masking pack for Oracle Enterprise Manager provides data masking capabilities. If you are using an MS SQL or DB2 RDBMS, then refer to the vendor documentation for information on data masking products.

Methods of Masking Data

When using a copy of production data for testing or development purposes, you have to mask sensitive data but also ensure that the original data is not changed so much in the masking process that it no longer allows a valid test of the functionality being verified.

The most appropriate method of masking data, without substantially changing it, varies according to the type of the data. The following are some methods that can be used for masking different types of data:

- **Numbers, such as credit card numbers and product numbers.** Rotate the numbers in the original data, and add a random value.
- **Dates and times.** Add or subtract a fixed amount of time to the original date or time value. Make sure that the result of the operation is still a valid date or time, and that start dates in the original data still occur before end dates in the original data.
- **Names, such as customer names or personal names.** Replace characters in names in the original data using a fixed or random substitution scheme. Be careful that the substitution does not increase the length of the resultant name values or buffer overflows can occur.
- **Status values, such as Active or Suspended.** Change each of the values to some other value picked from a list of known values. For example, a customer’s status can be changed from Active to Suspended, but not to Inactive if the term Inactive is not recognized by the application.

A

Supported Security Standards

This appendix provides information on the way in which Siebel Business Applications support the requirements of several security standards. It includes the following topics:

- Payment Card Industry Data Security Standard
- Common Criteria for Information Technology Security Evaluation
- Federal Information Processing Standard (FIPS) 140

Payment Card Industry Data Security Standard

The Payment Card Industry (PCI) Data Security Standard (DSS) is a set of standards developed to enhance the security of credit card data in organizations that process such data. Developed by the PCI Security Standards Council, the standards are designed to prevent credit card fraud by implementing consistent data-security measures, which include requirements relating to network management, security policies and procedures, and data-access management.

PCI DSS compliance is required of all organizations that store, process, or transmit credit cardholder data. The PCI DSS currently outlines six basic principles for compliance, supported by more detailed subrequirements for compliance.

Table A–1, " Siebel Business Applications and PCI DSS Requirements" lists the PCI requirements and the ways in which Siebel Business Applications support these requirements.

Note: Siebel Business Applications and features do not currently meet certain audit-related PCI DSS 3.1 compliance standards. The following PCI DSS 3.1compliance standard items are not covered by Siebel audit trail:

- System components.
- All actions taken by any individual with root or administrative privilege.
- Invalid logical access attempts.
- Use of and changes to identification and authentication mechanisms (including but not limited to new account creation and privilege elevation) and all changes, additions, or deletions to accounts with root or administrative privileges.

Table A–1 Siebel Business Applications and PCI DSS Requirements

PCI DSS Principle	PCI DSS Requirement	Siebel CRM Support for PCI DSS
Build and maintain a secure network.	Do the following: ■ Install and maintain a firewall to protect cardholder data. ■ Do not use vendor-supplied default passwords.	Siebel Business Applications support the deployment of firewalls, reverse-proxy servers, and Network Address Translation devices to protect application data from intrusion. During the installation of Siebel Business Applications, warnings are issued if the password specified for the user ID used to start services and processes is the same as the user ID. The installer can use any user ID and password that have the appropriate privileges to perform the task it is required to perform (such as administrator privileges to start services).
Protect cardholder data.	Do the following: ■ Protect stored cardholder data. ■ Encrypt transmission of cardholder data across open, public networks.	Siebel Business Applications allow customers to encrypt sensitive information stored in the Siebel database, cardholder data, and other data transmitted across networks.
Maintain a vulnerability management program.	Do the following: ■ Use and regularly update antivirus software on all computers commonly affected by malware. ■ Develop and maintain secure computer systems and applications.	These requirements are customer-governance issues. Oracle recommends that you implement them. For help with security-governance issues, contact your Oracle sales representative for Oracle Advanced Customer Services to request assistance.
Implement strong access control measures.	Do the following: ■ Restrict access to cardholder data by business need-to-know. ■ Assign a unique ID to each person with computer access. ■ Restrict physical access to cardholder data.	Siebel Business Applications provide multitiered access-control mechanisms so that only those users with appropriate rights have access to the data. This control includes view-level access control and record-level access control. Each Siebel application user is assigned a login ID, a primary position, and a responsibility in the Siebel application. These security attributes provide the user with the appropriate access rights to the Siebel application. Users do not have direct access to the Siebel database; only the Siebel application has access to it. To prevent users from circumventing application-security protocols if database security is used, then Siebel user passwords can be hashed using the RSA SHA-1 algorithm. Enabling password hashing makes sure that the password used to access the Siebel database is not the same password that the user uses to access the Siebel application. In addition, using an LDAP, ADSI, Single Sign-On, or custom-security adapter to access Siebel Business Applications requires that user database access is managed through a shared application credential, and not through a user ID and password.

Table A–1 (Cont.) Siebel Business Applications and PCI DSS Requirements

PCI DSS Principle	PCI DSS Requirement	Siebel CRM Support for PCI DSS
Regularly monitor and test networks.	Do the following: ▪ Track and monitor all access to network resources and cardholder data. ▪ Test security systems and processes regularly.	To maintain data continuity and monitor activity on a Siebel CRM site, you can configure Siebel Audit Trail. This feature allows you to maintain an audit trail of information that indicates when business component fields have been changed, who made the change, and what has been changed. These requirements are customer-governance issues. Oracle recommends that you implement them. For help with security governance concerns, contact your Oracle sales representative for Oracle Advanced Customer Services to request assistance.
Maintain an information security policy.	Maintain a policy that addresses information security.	This requirement is a customer-governance issue. Oracle recommends that you implement it. For help with security governance concerns, contact your Oracle sales representative for Oracle Advanced Customer Services to request assistance.

Common Criteria for Information Technology Security Evaluation

The Common Criteria for Information Technology Security Evaluation (Common Criteria) is an international technical standard that allows for security evaluations of computer products and technology. By providing an independent evaluation of a product's ability to meet specific security requirements, Common Criteria certification allows purchasers of IP products and technologies to make more informed decisions.

Siebel CRM version 7.8.2 obtained Common Criteria certification in January 2006. The security architecture of subsequent releases of Siebel CRM is unchanged from that release. The Validation Report for Siebel Business Applications Common Criteria certification is available on the Certified Products page of the Common Criteria Web site at

http://www.commoncriteriaportal.org/

For more information on Siebel CRM support for the Common Criteria standard, see 1363489.1 (Article ID) on My Oracle Support.

Federal Information Processing Standard (FIPS) 140

The United States government Federal Information Processing Standard (FIPS) 140 outlines the minimum security requirements for cryptographic modules (both hardware and software) that are used to protect sensitive information.

It is recommended that you verify that the cryptography module used in the applications in your implementation have FIPS 140-1 or FIPS 140-2 certification. The RSA BSAFE libraries used in Siebel Business Applications are FIPS 140-2 certified. Information on the standards supported by RSA BSAFE are available on the RSA BSAFE products page of the RSA Web site at

http://www.rsa.com/

B

Default Port Allocations

This appendix lists the default port allocations used by Siebel Business Applications. It includes the following topic:

- Port Allocations for Siebel CRM Release 8.x

Port Allocations for Siebel CRM Release 8.x

The port allocations that are assigned by default during the installation of Oracle's Siebel Business Applications for the Siebel Server and Siebel Web server are shown in Table B–1. It is recommended that you change the default ports used by these components.

> **Note:** In a Siebel Business Applications deployment, DNS servers use User Datagram Protocol (UDP) port 53 and Kerberos defaults to port 88.

Table B–1 Default Port Allocations for Siebel Business Applications

Siebel Component	Port Number	Comments
Web Server	80 and 443	Port 80 is used for standard Web traffic. If encryption is implemented, then port 443 is used.
Gateway Server	2320	Load-balancing components use port 2320.
Siebel Server	2321	SCBroker listens on port 2321. For information on SCBroker, see *Siebel System Administration Guide* and *Siebel Deployment Planning Guide*.
Siebel Server	49150 and higher (dynamic allocation of ports) 49149 and lower (static allocation of ports) 49152 to 49250 (dynamic ports listening on Siebel Servers)	Siebel Business Applications use dynamic allocation of ports for the server-based components. Static port allocation is also supported. The dynamic port allocation starts from port number 49150 onwards. If you choose to assign static ports to the components, then make sure that you choose ports below port number 49150. Dynamic ports can go up to port number 65535. These ports have to be opened on Siebel Servers. The Siebel system administrator allocates a port to a specific Siebel component.
Synchronization Manager	40400	None.

Table B–1 (Cont.) Default Port Allocations for Siebel Business Applications

Siebel Component	Port Number	Comments
Enterprise Application Integration (EAI) Server	Allocated by the system administrator.	Ports must be opened for the Siebel EAI and Workflow components. The Siebel system administrator allocates these ports.
SMTP Mail Server	25	None.
FTP Port	21	None.
Lightweight Directory Access Protocol (LDAP) Server	389 and 636	Port 389 is used for standard communications. Port 636 is used for secure communications.
Active Directory Server	389, 636, 3268, and 3269	Port 389 is used for standard communications. Port 636 is used for secure communications. Port 3268 is used for the Global Catalog and port 3269 is used for the Global Catalog with TLS.
Siebel Server or Siebel database	1521	Port 1521 is used for communications between the Siebel Server and Oracle database.
Siebel Server or Siebel database	1433	Port 1433 is used for communications between the Siebel Server and Microsoft SQL Server database.
Siebel Server or Siebel database	5000	Port 5000 is used for communications between the Siebel Server and IBM DB2 database for Linux, UNIX, and Windows.
File Server	139 Transmission Control Protocol (TCP) 137 and 138 User Datagram Protocol (UDP)	Port numbers for communications between the Siebel Server and the Siebel File System and Database Server are dependent on the file system type. The default TCP port number is 139. The default User Datagram Protocol (UDP) port numbers are 137 and 138.
Search Server	2048	None.

Index