Sage CRM Self Service

Securing Sage CRM Self Service

A Guide

Sage CRM Self Service enables businesses to create customer-facing websites that connect to their Sage CRM data.

Created: 26th March 2025

Step-by-Step IIS Security Configuration for Sage CRM Self-Service Sites

Enforcing HTTPS and Strong TLS

1.1 Obtain and Install an SSL Certificate

1. Obtain an SSL certificate from a trusted Certificate Authority (CA) or use Let's Encrypt for free certificates.
    - It is possible to use a PowerShell command to create a new self-signed digital certificate.
    - Example: New-SelfSignedCertificate -FriendlyName CRMSS -DnsName myservername -KeyUsage DigitalSignature
        1. New-SelfSignedCertificate: This is the PowerShell cmdlet to generate a self-signed certificate.
        2. -FriendlyName CRMSS: This assigns the friendly name "CRMSS" to the certificate. This name is used to easily identify the certificate in certificate stores.
        3. -DnsName myservername: This specifies the DNS name associated with the certificate. In this case, it's "myservername ". This is important for certificates used in network communications, as it ties the certificate to a specific domain or hostname.
        4. -KeyUsage DigitalSignature: This sets the intended usage of the certificate's private key. "DigitalSignature" means the key is intended to be used for digitally signing data, verifying the integrity and authenticity of information. It does not allow the certificate to be used for encryption.
    - **Note**: Self-signed digital certificates are useful for internal testing, development, and secure communication within private networks. However, they lack public trust, leading to security warnings, and are unsuitable for public-facing websites or applications handling sensitive data.

2. **Installing a Digital Certificate on IIS for a Self Service site e.g. CRMSelfServicedemo:**
    - **Import the Certificate**:
        1. Open mmc.exe (Microsoft Management Console).
        2. File > Add/Remove Snap-in... > Certificates > Add > Computer account > Local computer > Finish > OK.
        3. Navigate to Certificates (Local Computer) > Personal > Certificates.
        4. Right-click Certificates > All Tasks > Import....
        5. Browse to your certificate file (.pfx or .p12).
        6. Enter the certificate password.
        7. (Optional) Check Mark this key as exportable.
        8. Let it automatically select the certificate store.
        9. Click finish.
    - **Bind the Certificate to CRMSelfServicedemo in IIS:**
        1. Open inetmgr.exe (IIS Manager).
        2. Expand your server name > Sites > CRMSelfServicedemo.
        3. In the Actions pane, click Bindings....
        4. Click Add....
            1. Type: https.
            2. IP address: Your server's IP or All Unassigned.
            3. Port: 443.
            4. SSL certificate: Select the imported certificate.
        5. Click OK > Close.
    - **Verify the Installation:**
        1. Open a web browser and go to https://yourdomain/CRMSelfServicedemo.
        2. Look for the padlock icon and ensure no security warnings appear.
        3. Clear browser cache if there are any issues.
3. **Key Reminders:**
    - **Firewall**: Ensure port 443 is open on your Windows Firewall.
    - **DNS**: The DNS record for your domain must point to the server's IP.
    - **Certificate validity**: Check the certificate's expiration date.
    - If you have issues locating the certificate, review the certificate store within the MMC snap in.

Enforce HTTPS Redirection

Using URL Rewrite (Recommended)

1. Install the URL Rewrite Module (if not already installed).
2. Open IIS and select the Self-Service site.
3. Navigate to: *URL Rewrite* > *Add Rules* > *Blank Rule*.
4. Configure the rule as follows:
    - **Match URL**:
        - Requested URL: *Matches the Pattern*
        - Using: *Regular Expressions*
        - Pattern: (.*)
    - **Conditions**:
        - Condition input: {HTTPS}
        - Check if input string: *Matches the Pattern*
        - Pattern: ^OFF$
    - **Action**:
        - Action type: *Redirect*
        - Redirect URL: https://{HTTP_HOST}/{R:1}
        - Redirect type: *Permanent (301)*
5. Click Apply to save the changes.

Configure Strong TLS Settings

1. Download and install **IIS Crypto** (**https://www.nartac.com/Products/IISCrypto**).
2. Run IIS Crypto as Administrator.
3. Select **Best Practices** or customize settings:
    - **Enable:** TLS 1.2
    - **Disable:** SSL 3.0, TLS 1.0, TLS 1.1.
    - **Disable weak ciphers** (such as RC4, DES).
4. Click **Apply** and restart the server.

1.4 Implement HTTP Strict Transport Security (HSTS)

1. In IIS Manager, select the **Self-Service** site.
2. Click **HTTP Response Headers**.
3. Add a new header:
    - Name: Strict-Transport-Security
    - Value: max-age=31536000; includeSubDomains
    - (Optional but recommended: Add ; preload if you plan to submit the site to the HSTS Preload List.)
4. Click OK to save the changes.

IIS Hardening

2.1 Keep IIS Patched

1. Regularly install **Windows Server updates**.
2. Apply security patches as soon as they are available.

2.2 Disable Unnecessary Features

1. Open **Turn Windows features on or off**.
2. Disable any **unused IIS roles or features**, such as:
    - **WebDAV Publishing**
    - **Anonymous Authentication** (if not required)

2.3 Configure Firewall Rules

1. Open **Windows Firewall**.
2. **Allow only necessary traffic**:
    - **Allow:** HTTPS (443), HTTP (80, only if redirecting to HTTPS).
    - **Block:** All other inbound and outbound traffic unless explicitly required.

2.4 Enable Request Filtering

1. In IIS Manager, select the **Self-Service** site.
2. Click **Request Filtering**.
3. Configure as needed:
    - **Restrict file extensions** (e.g., deny .exe, .bat, .cmd if not required).
    - **Set maximum request length** to prevent large file uploads.

2.5 Configure IP Address Restrictions

1. **Install the IP and Domain Restrictions Module** (if not already installed)
    1. Open Server Manager > Click Manage > Select Add Roles and Features.
    2. In the Features section, select IP and Domain Restrictions, then install it.
2. **Configure IP Restrictions**
    1. Open IIS Manager and select the **Self-Service** site.
    2. Click IP Address and Domain Restrictions. (If it's missing, ensure the module is installed.)
    3. In the Actions pane, click Add Allow Entry or Add Deny Entry:
    4. To allow an IP: Enter the IP address or range, then click OK.
    5. To deny an IP: Enter the IP address or range, then click OK.
    6. Click Edit Feature Settings in the right panel to configure behaviour:
        1. Deny Access by Default: Select "Deny" if you want to block all traffic except allowed IPs.
        2. Allow Access by Default: Select "Allow" if you only want to block specific IPs.
    7. Enable Deny Action Type (Forbidden, Not Found, Abort, etc.).
    8. Apply and Test the Configuration
        1. Click Apply to save changes.
    9. Test access from an allowed and denied IP to verify restrictions.

2.6 Enable Logging and Auditing

1. In IIS Manager, select the **Self-Service** site.
2. Click **Logging**.
3. Ensure logs capture **failed login attempts and access to restricted resources**.
4. Review logs regularly using **Windows Event Viewer**.

Application Pool Configuration

3.1 Use a Least Privileged Account

1. Create a **dedicated service account** for the self-service application pool.
2. Grant only **necessary permissions**.
3. In IIS Manager, select **Application Pools** > **Self-Service Pool**.
4. Click **Advanced Settings** > Change **Identity** to the service account.

3.2 Configure Application Pool Recycling

1. In IIS Manager, select **Application Pools**.
2. Click **Advanced Settings** on the **Self-Service Pool**.
3. Set regular recycling intervals to prevent memory leaks.

4.1 Prevent Clickjacking (X-Frame-Options)

1. In IIS Manager, select the **Self-Service** site.
2. Click **HTTP Response Headers**.
3. Add:
    - Name: X-Frame-Options
    - Value: SAMEORIGIN (or DENY if embedding is not needed).

4.2 Prevent MIME Sniffing (X-Content-Type-Options)

1. Add:
    - Name: X-Content-Type-Options
    - Value: nosniff

4.3 Implement Content Security Policy (CSP)

1. Add:
    - Name: Content-Security-Policy
    - Value: default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; img-src 'self' data:
    - Adjust based on the self-service site's needs.
2. Test in **report-only mode** before enforcing.

Additional Considerations for Sage CRM Self-Service

- **Authentication & API Security:**
    - Ensure **API credentials are not exposed in client-side code**.
    - Verify that API requests use **secure authentication methods**.
- **Session Management:**
    - Configure session timeouts to prevent unauthorized access.
    - Ensure Sage CRM **session management works correctly** when IIS recycles the app pool.
- **Performance Testing:**
    - After implementing security measures, test API **response times** to ensure they are not negatively impacted.

Final Testing Steps:

- ☑ Verify **HTTPS redirection** and enforce TLS 1.2
- ☑ Check IIS **logging and request filtering settings**.
- ☑ Ensure **self-service site functions correctly** after applying security changes.
- ☑ Confirm that **API calls to Sage CRM work securely**.
- ☑ Validate **session handling and authentication mechanisms**.
- ☑ Run security scans using **securityheaders.com** or similar tools.

Always test these changes in a staging environment before applying to production.