Security hardening on-prem and the service

Kennie Nybo Pontoppidan
Jens Møller-Pedersen
Who are we?

Kennie Nybo Pontoppidan (keponent@microsoft.com)
Server Program Manager

Jens Møller-Pedersen (jensmp@microsoft.com)
Server Lead Engineer
Objectives

1. Refresh what you already know about application security
2. Deep dive into all the other security matters you must consider
3. Get confident why Business Central is a platform you can trust
Disclaimer

This presentation is provided for informational and training purpose only. It represents Microsoft’s view as of the presentation date. Microsoft cannot guarantee the accuracy of any information after the presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted as a commitment on Microsoft’s part. This presentation is provided “as-is”.

Sample code included in this presentation is made available AS IS.

© Copyright Microsoft Corporation. All rights reserved
What is hardening?

“... the process of securing a system by reducing its surface of vulnerability”

https://en.wikipedia.org/wiki/Hardening_(computing)
The onion model

Aka
• Defense in Depth
• Layered Security
Assume breach

Assume Breach limits the trust placed in applications, services, identities and networks by treating them all—both internal and external—as not secure and probably already compromised.
## Security Overview

You can use the following table as a checklist to help set up a more secure Dynamics NAV environment.

<table>
<thead>
<tr>
<th>To</th>
<th>See</th>
</tr>
</thead>
</table>
| Install Dynamics NAV software. | You must make decisions about where you install Dynamics NAV components.  
|  | Working with Microsoft Dynamics NAV Setup |
| Activate your Dynamics NAV license. | How to: Upload the License File |
| Create users. | How to: Create Microsoft Dynamics NAV Users |
| Assign users to permission sets. | How to: Define Permissions for Users |
| Configure Role Centers. | Profiles and Role Centers |
| Assign users to profiles. | Managing Users |
Application security
The gold standard for security (they all begin with Au)

- Authenticating
- Authorizing
- Auditing
### Authentication consideration

Establishing the identity of a user

<table>
<thead>
<tr>
<th>Method</th>
<th>Benefits</th>
</tr>
</thead>
</table>
| Windows             | • Easy and secure for on-premise installation  
                        • Works out of the box                                                  |
| Azure AD            | • Integration with cloud services and Office 365  
                        • Strong password management / 2 Factor Authentication  
                        • Some setup is needed*                                                  |
| Web Access Key      | • Create specific ‘synthetic’ user with limited permissions  
                        • ‘No’ password management                                               |
| NavUserPassword     | • Another password to remember  
                        • Management is up to the BC administrator                               |

# Layered authorization system

Specifying access rights to resources

<table>
<thead>
<tr>
<th>TestPermissions</th>
<th>• Extra layer added in test</th>
</tr>
</thead>
</table>
| Permissions      | • Union of permission sets assigned  
                  | • Highest permission wins        |
| Entitlements     | • Union of entitlement set assigned  
                  | • Highest entitlement wins       |
| License          | • Shared license for all users  
                  | • Indirect permissions can limit access |
Copying system permission sets
Effective permissions
Where do users get permissions from?

- BC User Group memberships
- Permission Sets assigned directly
- Windows security groups
- CSP partner role

https://docs.microsoft.com/en-us/dynamics-nav/managing-user-groups
Auditing

...the decisions of the guard, so that later it’s possible to figure out what happened and why
Auditing data changes

Change log
Auditing security changes

Change Log is always enabled for changes to security tables

Use Change Log setup to add further tables
SQL Server auditing - track and log events that occur on the Database Engine

Who accessed your sensitive tables in the last week?

What has your administrator changed in the past month?

Server level auditing – all editions

Database level auditing - only Enterprise edition
Environment security
Components to harden

Client
Server
Database
Network
Configuring SSL to Secure the Connection to Dynamics NAV Web Client

We recommend that you secure Dynamics NAV data that is transmitted over the internet by enabling Secure Sockets Layer (SSL) on the connection to Microsoft Dynamics NAV Web client.

SSL is a web protocol that encrypts data that is transmitted over a network to make the data and the network more secure and reliable. A website that is enabled with SSL uses Hypertext Transfer Protocol Secure (HTTPS) instead of Hypertext Transfer Protocol (HTTP) as a communication protocol. Enabling SSL on a website requires that an SSL certificate is installed on the web server. An SSL certificate is a small file that the web server uses to prove its identity and establish a trusted connection with the browser that is trying to access Microsoft Dynamics NAV Web client. When a browser connects to the Microsoft Dynamics NAV Web client, the web server replies by sending its certificate to the browser. This certificate contains the web server’s public encryption key and the name of the authority that granted the certificate. The browser verifies the certificate using the authority’s public key.

To configure SSL, you must follow these steps:

- Obtaining an SSL Certificate
- Adding an HTTPS Binding That Uses the Certificate on the Microsoft Dynamics NAV Web Client Site
- Redirecting HTTP to HTTPS (Optional)

Note

You can configure SSL for the Microsoft Dynamics NAV Web client when you install the Microsoft Dynamics NAV Web Server components. For more information, see How to Install the Web Server Components.
OData over HTTP vulnerability

- Credentials can be exposed if http traffic is intercepted
- **Always** use SSL to avoid this condition, i.e. an https endpoint
- Use real certificates and consider revocation process
- Only roll your own for **test environments**

- For more information, see
  - Walkthrough: Configuring Web Services to Use SSL (SOAP and OData)
  - Configuring SSL to Secure the Connection to Dynamics NAV Web Client
  - How to: Implement Security Certificates in a Production Environment
Server hardening

Service accounts

Limit Port Access
- Port 7046
- Port 1443
- (Port 443)
Using multiple NSTs for stability

- Separate NST for external users
  - Only SOAP and OData endpoints exposed

- Dedicated NST for running job queues
  - Avoid slowing down user sessions

- Consider using different service account
Configuring Microsoft Dynamics NAV Server

When you run Microsoft Dynamics NAV 2018 Setup and install Microsoft Dynamics NAV Server, you provide information that is then used as the configuration for the default Microsoft Dynamics NAV Server instance. This information is stored in a configuration file for the server instance called CustomSetting.config. The default location of the CustomSettings.config file is C:\Program Files\Microsoft Dynamics NAV\NAVService.

After you install Microsoft Dynamics NAV Server, you can change any of the settings that you provided during Setup, plus several other settings that were not available to you in Setup.

**Note**

Each Microsoft Dynamics NAV Server instance has its own CustomSettings.config file.

Configuring Microsoft Dynamics NAV Server in Setup

You configure the default Instance of Microsoft Dynamics NAV Server by running Microsoft Dynamics NAV 2018 Setup and selecting one of the following Installation Options:
Locking down other server settings

- ReportAppDomainIsolation
- ClientServicesMaxUploadSize
- RestrictedFileTypes
- EnableDataExportImport
- EnableALServerFileAccess
- DebuggingAllowed
- EnableDebugging

- Use domain isolation for running custom RDLC layouts
  - Can contain .Net references
  - Will cause reports with custom RDLC to run slower

- Limit file uploads
  - Restrict types of files
  - Limit the size of files

- Limit what code can do

- Turn off what you don’t need
  - Debugging
In Server MMC console:
select the *Enable SSL* check box under *SOAP Services and OData Services*
Power BI integration

Always use HTTPS url to connect to server

Connect to Microsoft Dynamics NAV with Power BI

Getting insights into your Microsoft Dynamics NAV data is easy with Power BI. Power BI retrieves your data, both Sales and Financial, then builds an app with a dashboard and reports based on that data. Power BI needs your permissions to the tables where data is retrieved from, in this case sales and finance data. More details on requirements below. After you install the app, you can view the dashboard and reports in the Power BI service (https://powerbi.com), and in the Power BI mobile apps.

Connect to the Microsoft Dynamics NAV for Power BI or read more about the Dynamics NAV integration with Power BI.

How to connect

1. Select Apps in the left navigation pane > select Get apps in the upper-right corner.
SQL Server hardening

Gold standard

BC is not vulnerable to SQL injection
Database user privileges

<table>
<thead>
<tr>
<th>NST runtime</th>
<th>NST sync</th>
<th>BI/DW</th>
</tr>
</thead>
<tbody>
<tr>
<td>db_reader</td>
<td>db_reader</td>
<td>db_reader</td>
</tr>
<tr>
<td>db_writer</td>
<td>db_writer</td>
<td></td>
</tr>
<tr>
<td>alter table</td>
<td>ddl_admin</td>
<td></td>
</tr>
</tbody>
</table>

Transparent Data Encryption (TDE)

In May 2018 we declared support for Transparent Data Encryption (TDE) on SQL Server.

Available in SQL Server Enterprise Edition and Azure SQL Database.

TDE performs real-time I/O encryption and decryption of the data and log files to protect data at rest.
Transparent Data Encryption (TDE)

You can use Transparent Data Encryption (TDE) to encrypt SQL Server and Azure SQL Database data files at rest. In a scenario where the physical media (such as drives or backup tapes) are stolen, a malicious party can just restore or attach the database and browse the data. With TDE you can encrypt the sensitive data in the database and protect the keys that are used to encrypt the data with a certificate. TDE performs real-time I/O encryption and decryption of the data and log files to protect data at rest. TDC can assist in the ability to comply with many laws, regulations, and guidelines established in various industries.

**Important**

TDE does not provide encryption across communication channels. For more information about how to encrypt data across the communication channel between the database and the Microsoft Dynamics NAV Server, see [Enhancing Microsoft Dynamics NAV Server Security](#).

**Caution**

Backup files of databases that have TDE enabled are also encrypted by using the database encryption key. As a result, when you restore these backups, the certificate protecting the database encryption key must be available. This means that in addition to backing up the database, you must make sure that you also maintain backups of the server certificates to prevent data loss. Data loss will result if the certificate is no longer available.
TLS 1.2 support for Microsoft SQL Server

Applies to: SQL Server 2008 Developer, SQL Server 2008 Enterprise, SQL Server 2008 Express, More

Introduction

This article provides information about the updates that Microsoft is releasing to enable TLS 1.2 support for SQL Server 2017 on Windows, SQL Server 2016, SQL Server 2008, SQL Server 2008 R2, SQL Server 2012, and SQL Server 2014. This article also lists supported client providers.

Several known vulnerabilities have been reported against SSL and earlier versions of Transport Layer Security (TLS). We recommend that you upgrade to TLS 1.2 for secure communication.
Other security issues
Backups

Use backup encryption
Know your partners’ code

- .Net interop is a very powerful tool
  - Access to files on the machine
  - Thread dispatcher cannot control the flow
  - Reflection can allow looking at in-memory structures
  - Static variables can cause tenants to affect each other

- Don’t add .Net components you do not trust
- Protect your hardware using Hyper-V containers

- .Net interop not allowed in Business Central extensions
Hardening the users

Attackers will use the easiest way to get access
Mind the baby... (0:22)

And I can't remember what email address we used to log on to the account, and the baby's crying--
What’s your password? (0:42)
Service security
What do we (Microsoft) do?

Secure Development Lifecycle (SDL)

Software development process that helps developers build more secure software and address security and privacy compliance requirements.

The SDL includes

- Risk assessments
- Attack surface analysis and reduction
- Threat modeling
- Incident response
- Release review and certification

https://www.microsoft.com/en-us/sdl
Top security certifications

Compliance by service

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 27001</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ISO 27017</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ISO 27018</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Cross Industry</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SOC 1 (SSAE 18) Type 2</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SOC 2 Type 2</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>PA-DSS</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>✓</td>
<td>✓</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>CSA STAR Self-Assessment</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Health</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIPAA BAA</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Manufacturing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FDA CFR Title 21 Part 11</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Government</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EU-US Privacy Shield</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>EU Model Clauses</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>UK Official</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Spain ENS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Spain LOPD</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>FINMA (Swiss, FSI)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>FERPA</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

https://aka.ms/d365-compliance-list
Encryption everywhere

- Encryption at rest (databases are encrypted using TDE)
- Encryption in transit (all services use encrypted protocols, e.g. HTTPS)
- Encryption in memory (.net secure strings for connection strings)
- Encrypted backups
VM security

Running NST in container in our ISV embed program
Secure Admin Workstation (SAW)
JIT access to production environments
Azure VM security

Azure Security Pack
• Alerts if running non-signed bits
• Alerts if suspicious OS kernel activity
Microsoft Cyber Defense Operations Center

Staffed with dedicated teams 24x7, the Center has direct access to thousands of security professionals, data scientists, and product engineers throughout Microsoft to ensure rapid response and resolution to security threats.