In this topic we will cover the security functionality provided with SAP Business One.
After completing this topic, you will be able to:

- Describe the security functions provided by the System Landscape Directory
- Set up single sign-on for access to SAP Business One using Windows domain credentials
- Change the site user password
- Change the database admin user for a company database
- Manage and change user passwords
- Create a read-only database user
- Describe the information logged in the Access and Change history logs
When you implement SAP Business One, you should ensure that you take all steps to safeguard the customer’s information.

SAP Business One provides multiple features for implementing security measures, and you should work together with the customer to determine which options will best meet the customer’s security requirements.
The first part of this topic covers the security features provided in the System Landscape Directory.
When a user logs on to an SAP Business One company, the user’s credentials are validated by the **System Landscape Directory** service, and after they have been validated the client then connects to the company database using the database credentials. Therefore security is maintained since database credentials are hidden from the end user.

The security landscape directory service (SLD) is responsible for authenticating the users’ logon credentials. Therefore SAP Business One users do not connect directly to the database, but receive access credentials from the SLD.
The System Landscape Directory (SLD) provides a secure web interface for an administrator to manage the overall landscape of a system, including servers and company databases.

We will examine some of the functions provided in the SLD.
The SLD server is installed as part of the SAP Business One server tools. To access the SLD, open the License Manager service in the Service Manager. Open the General Settings screen then select Configure Security. The System Landscape Directory will open up in a Web browser.

You can also enter the url https://localhost:30010/ControlCenter in a Web browser on the SAP Business One server.

The SLD enforces a secure connection using HTTPS protocol. During the installation you are given the choice of installing a purchased third-party security certificate (PKCS12) or self-certifying that the connection is secure. If you choose to self-certify, you will get a warning from the Web server, and you can ignore the warning to continue to the site.

Access in two ways:
- Open License Manager settings and select Configure Security, or
- Enter url in Web browser
  https://localhost:30010/ControlCenter

Note: Web browser must be on same machine as license server

Need to install security certificate or self-certify
You need to enter the site user password to proceed to access the SLD. On the Security Settings tab of the SLD, you can change the site user password.

The site user password is required to create new companies and to upgrade companies. To maintain security for the landscape, the customer should change the site user password regularly.
If the site user password is forgotten, you can reset it from the SLD. You need to provide the database admin name and password, and then supply a new password for the site user.
The SLD also allows the administrator to manage the authentication mode. There are two types of logon authentication:

- **SAP Business One Managed Authentication** – Each SAP Business One user can access a company database using their user account code and password that is managed from within SAP Business One.

- **Windows Authentication** – Each SAP Business One user can access a company database using their windows domain account (single sign on).

Whichever logon method is used, internally the user identity is the same. Single sign on allows users to bypass the standard SAP Business One login screen. If the user has already logged into the windows domain, they do not need to login again to SAP Business One.

To use single sign on, you must first enable it in the System Landscape Directory. Once set, this applies to all companies on all servers in the landscape.
To enable single sign-on for a user, you must bind the user’s SAP Business One user account with the user’s Windows domain account. This is a one-to-one mapping between the user account and the Windows account. The domain user name (without domain) will be used as the user code. The user’s client machine must be in the same domain as the server.

For security reasons, the bind between the SAP Business One user account and the domain user cannot be changed once established.
After the user account is bound, the user can then select a checkbox on the SAP Business One login window and start using the application without being prompted to enter their SAP Business One logon credentials.

If the user’s machine is not in the same domain, the checkbox is not selectable. The user can still login using their SAP Business One account by unchecking the checkbox in the Choose Company screen.

The first time a user selects the checkbox on the Choose Company screen, the user is prompted to provide their SAP Business One account code and password. Once this is provided, no further prompting occurs and subsequently the user does not have to login to SAP Business One. The logon screen will not appear for the next login, instead SAP Business One will be launched directly with the last company and current domain user.

If there are multiple company databases on the server, the Choose Company window will only display companies in which the user account is bound with the domain. Therefore if a user needs to access two companies, you need to bind the user account in each company.
On the Servers and Companies tab, the SLD displays the server specified in the installation, and the company databases on the server. You can add new servers to the landscape (post installation), and remove servers from the landscape.

You can edit the server to set the type of authentication as either SQL Server authentication or Windows authentication. Note that SAP recommends using SQL Server authentication. For more information, consult the SAP Business One Administrator’s Guide.
Also on the Servers and Companies tab, you can change the default database account (typically “sa”) that is used by the client for access to all company databases. This user account has system admin privileges which are not needed for SAP Business One access.

So for enhanced security, you can change to a database user with fewer admin privileges. Select and edit a company database, and, in the pop-up window, select the option *Use Specified Database User* instead of the default *Use Database Admin User*. A new user account is automatically generated on Microsoft SQL Server and the company database is mapped to this new account. The database user account is now displayed in the row in the SLD. You can maintain the password for this account using SQL Server Management Studio.
In this demo, we will show the security functions in the System Landscape Directory.
The next part of this topic focuses on the administration of user passwords.
You can configure a global password policy for all users, which will dictate the strength of the user password and how often it needs to be changed. To change the password policy from the default, choose Administration → Setup → General → Security → Password Administration. Here you can set the password strength (low, medium, high, or custom) and any special requirements for characters that need to be part of the password.

When a new user is created, an initial password is set by the administrator. The new password must adhere to the password strength defined in the Password Administration screen.

If single-sign on is in use throughout the company, the user still has the option to login using their SAP Business One credentials, so the password policy should be maintained.
Users can change their password at any time by choosing the menu
Administration → Setup → General → Security → Change Password.

The super user change the password for another user by selecting the browse button in the user account. The super user should inform the user so they can login successfully using the new password.

The super user also has the option to force a user to change their password when they next login, by selecting the Change Password at Next Logon checkbox in the user account.

Users can change their password at any time by choosing the menu
Administration → Setup → General → Security → Change Password.

Super user can change password for another user and force user to change password at next logon.
A user account can be locked to prevent the user from logging on to SAP Business One. The super user can lock an account manually, and the account will be automatically locked after a specified number of unsuccessful login attempts by the user, if this is defined in the password policy. The default password policy does not lock a user account. Only a superuser can unlock a user account.
In order to prevent illegal updates to the database, you can restrict users to read-only operations on the database.

First you need to set up a read-only user account in the Microsoft SQL Server database. Map the user account to the SBO-Common and company database. Select the role memberships as `db_datareader` and `db_denydatawriter`.

Next, in SAP Business One, choose Administration > Setup > General > Read-Only DB User. Enter the read-only user name and password.

Users are now restricted and will not be able to run SQL update or delete queries unless they are assigned the general authorization Reports > Query Generator > Execute Non-select SQL Statement.

For more information, see the Administrator's Guide.

Only SAP Business One super users are able to specify read-only users.
Demo – Password Administration
The final part of this topic covers the access and change logs provided in SAP Business One.
An audit log is maintained that records each user logon, logoff, and password change. This is especially useful for monitoring password changes and failed login attempts.

To view the log, choose the *Tools* menu then choose *Access Log*. You can double-click a row to see details for a user. The IP address is included in the details, allowing the administrator to track the source of an attempted login.
The change log records changes in many objects, including sales and purchasing documents, and setup windows such as tax groups, withholding tax, house banks, freight, credit cards, general authorizations, general settings, document settings, employee master data, production orders, and the charts of accounts.

To determine if a window has a change log, open the document or form and choose **Tools > Show History**. This menu option will only be active if the document or form in the active window has a change log.

The change log shows a row for each change made to the document or window. When a document is first added, the change log shows one row. If the document is subsequently changed, the change log will show an additional row for each change.
If you choose *Show Differences*, you will see a detailed comparison of each field with the field differences highlighted.

If you double-click the first row you will see a saved image of the document before the change was made. If you double-click the second row you will see a saved image of the document with the change, and so on.

Note that the maximum number of rows that can be recorded for a document or window is set in the *General Settings > Services* tab, in the *History* field. The default is 99 rows.
This demo will show the access and change logs.
Here are some key points to take away from this session:

- When a user logs on, user credentials are validated by the System Landscape Directory (SLD). After they have been validated, SAP Business One users do not connect directly to the database, but receive access credentials from the SLD.
- The SLD provides a web interface for managing the overall landscape as well as security.
- The SLD can be accessed from the License Manager settings or using the url `https://localhost:30010/ControlCenter`.
- From the SLD you can change the site user password, enable single-sign on, add servers to the overall landscape, and change access credentials to the database.
- A super user can set a password policy for users, change a user password, and lock a user account.
- Access and change logs provide useful information for managing security.
Thanks!

You have completed the topic for security in SAP Business One.

Thank you for your time!