Overview of SQL Security Manager

SQL Server for Windows NT can be set up (using the setup program) with three different types of login security: standard, integrated, and mixed.

- With standard login security, SQL Server users must specify a login ID and a password to access the server.
- With integrated security, SQL Server uses Windows NT security to authenticate users; users do not have to maintain separate SQL Server login passwords. Integrated security is available only for clients connecting using the default named pipes protocol.
- With mixed security, if your SQL Servers are set up to accept different network protocols in addition to named pipes, you can take still advantage of integrated security features for the named pipes clients. Mixed security allows users who are using either standard or integrated security to access SQL Server. Mixed security allows anyone to access SQL Server if they have a valid SQL Server login ID and password; authorized Windows NT accounts can also connect to SQL Server with through named pipes without supplying a SQL Server login ID and password.

SQL Security Manager provides a graphical way to map Windows NT users and groups to SQL Server login IDs for integrated or mixed security. If you are using standard security, you must use Microsoft SQL Administrator or Transact-SQL statements to set up login IDs.

SQL Security Manager also allows you to grant and revoke SQL Server privileges to Windows NT groups, including setting up SQL Server login IDs and passwords for the group and adding users to SQL Server databases. In addition, you can use SQL Security Manager to search for the SQL Server access permissions for a given Windows NT account.

Windows NT groups that have access to SQL Server are displayed in a hierarchical tree by group. You can double-click the group name to expand the tree and view all users in the group. To view a user's account information, double-click the username. You can view groups with either user privilege or system administrator privilege.

Related Topic

Setting Up Accounts with the Windows NT User Manager

Setting Up Accounts with the Windows NT User Manager

In order to take advantage of integrated or mixed security for SQL Server, you must first create Windows NT groups and add users to those groups. When Windows NT is installed, an Administrators group is created. By default, all users added to the Administrators group are given system administrator privilege (sa) on the SQL Server.

The following hints will help you smoothly set up accounts with the Windows NT User Manager that can then be mapped to SQL Server login IDs:

- Create one administrator-level group and one or more user-level groups for the accounts that will access SQL Server. The groups should correspond to the security levels that you want to grant in your SQL Server databases (for example, OrderEntry and OrderEntryManagers). If you want your Windows NT administrators to be the same users as your SQL Server system administrators, you can leave the default permissions created by the setup program. Otherwise you can create a separate group for SQL Server administrators and grant that group administrative privilege both on Windows NT and on SQL Server. After you create a separate administrator group for SQL Server system administrators, it is a good idea to revoke privilege from the Windows NT Administrators group.
- When you create names for Windows NT users and groups it is advisable to use only valid SQL Server identifiers. Do not use spaces, periods, or other characters that Windows NT allows but SQL Server doesn't, and do not exceed 30 characters for group names. In addition, do not use the underscore (_), dollar sign ($), or pound sign (#) in the user or group names because these characters are used by SQL Server as special mapping characters.
- Avoid placing Windows NT users in more than one Windows NT group that can access SQL Server, because SQL Server does not allow overlapping group membership within databases. Keeping your Windows NT users limited to one group will allow you to use SQL Security Manager to keep database groups consistent with Windows NT groups.

Related Topics

Overview of SQL Security Manager

Granting Privileges

Logging In to a SQL Server

Before you can use SQL Security Manager, you must log in to the SQL Server that you are managing integrated security accounts for. When you first start SQL Security Manager, the Connect Server dialog box appears automatically. You can also choose to connect to another SQL Server at any time, but you can be connected to only one SQL Server at a time.

To log in to a SQL Server

1. From the File menu, choose Connect.

   The Connect Server dialog box appears.
2. In the Server box, select or type the name of a server.

   The Server box contains a list of the last 5 servers logged in to. To get a list of servers on the network, choose the List Servers button.
3. In the Login ID box, type your login ID. Then, in the Password box, type your password.

   Note that if you are using integrated security, you do not need to supply a login ID or password.
4. Choose the Connect button.

   If the server you connect to is running in standard security mode, you will get a message stating that SQL Security Manager cannot be used on that server. To change your security mode, use the Set Security Options dialog box in the SQL Server setup program.

Configuring SQL Security Manager

You can change configuration options that: set timeouts for login attempts and for retrieving query results, set automatic ANSI to OEM character conversion, or set an option so that when you drop a user with the SQL Security Manager, a search is performed to determine if the user is a member of multiple groups that have access permission. This option will help find unexpected problems that might occur when users have overlapping group memberships, but it will also slow down all drop operations.

To configure SQL Security Manager

1. From the File menu, choose Configure.
   The Configure SQL Security Manager dialog box appears.
2. Set the appropriate configuration options.
3. Choose the OK button.

To set all options to their default values

- Choose the Defaults button.

Viewing Users with User Privilege

When SQL Security Manager is open, a tree displaying the groups added to SQL Server is displayed. You can choose between viewing groups with user privilege and groups with system administrator privilege.

To view users with user privilege

- From the View menu, choose User Privilege.

  The groups with user privilege are displayed in the window. To view information about the individual members of a group, double-click the group name. To view details about an individual user's account, double-click the username. To view details about a group account, double-click the group name while pressing the CTRL key. To collapse the list of usernames, double-click the group name again.

Related Topic

Viewing Users with System Administrator Privilege

Viewing Users with System Administrator Privilege

When SQL Security Manager is open, a tree displaying the groups added to SQL Server is displayed. You can choose between viewing groups with user privilege and groups with system administrator privilege.

To view users with system administrator privilege

- From the View menu, choose SA Privilege.

  The groups with system administrator privilege are displayed in the window. To view information about the individual members of a group, double-click the group name. To collapse the list, double-click the group name again. All users with system administrator privilege access SQL Server using the SA login ID so there are no account details for these accounts.

Related Topic

Viewing Users with User Privilege

Granting Privileges

When you grant privileges to a Windows NT group, you are granting access to SQL Server to each member of that group. You can grant either user privilege or system administrator privilege.

To grant user privilege

1. From the View menu, choose User Privilege.
2. From the Security menu, choose Grant New.

   The Grant User Privilege dialog box appears.
3. In the Grant Privilege box, select the group that will have access to SQL Server.

   To show all local groups on the Windows NT-based computer, choose Local Groups. To show all groups on the default domain, select All Groups on the Domain.
4. The Add login IDs for individual group members box is selected. This specifies that you want to create SQL Server login IDs for each user in the group.

   If you do not want each user in the group to have a separate SQL Server login ID, clear the check box. If you do not assign each user an individual login ID, the only way the user can access SQL Server is through the default login ID (usually "guest"). If you want to set up security like this, be sure you've added a guest account when you set security options with the SQL Server setup program.
5. To add users in the group to a database, so that database is their default database when they log in to SQL Server, select the Add Users to Databases box, and then select the database. It is recommended that you assign users to another default database other than *master*, to discourage users from creating database objects in *master*. If you do not assign users to a default database, *master* becomes their default database.
6. Choose the Grant button.

To grant system administrator privilege

1. From the View menu, choose SA Privilege.
2. From the Security menu, choose Grant New.

   The Grant System Administrator Privilege dialog box appears.
3. In the Grant Privilege box, select the group that will have access to SQL Server.

   To show all local groups on the Windows NT-based computer, choose Local Groups. To show all groups on the default domain, select All Groups on the Domain.

   Note that when you grant system administrator privilege, the Add Login IDs and Add Users to Database boxes are dimmed. This is because when you grant to a group system administrator privilege to SQL Server, the users in the group are automatically mapped to the SA login ID and *master* is the default database.
4. Choose the Grant button.

NOTE: If you grant permission to the "Domain Users" group on the default domain, you will see as domain members all of the Windows NT computer accounts (ending in a "$") in addition to all of the user accounts defined on the domain. Since computer accounts do not need SQL Server login permissions, it is a better idea to create a separate group on the domain containing only the valid user accounts, then grant permission to this group.

Related Topics

Revoking Privileges

Getting Details About an Account

Revoking Privileges

When you revoke privileges, all users in the group that you are revoking permission from are dropped from SQL Server databases and their login IDs removed from SQL Server.

To revoke privileges

1. From the View menu, choose User Privilege or SA Privilege.

   The groups with that privilege are displayed.
2. Click the name of the group to revoke privilege from.
3. From the Security menu, choose Revoke.

   A confirmation message appears.
4. Choose Yes.

   If you want to deny SQL Server access to a member of a group with SQL Server privilege, use the Windows NT User Manager to remove the user from the group. The SQL Server login ID and any database usernames associated with that Windows NT account will remain in SQL Server but will be inaccessible to that user. You can periodically clean up these login IDs and usernames by using the Find Orphan SQL Login IDs option in the Search for Account Information dialog box.

Related Topics

Granting Privileges

Getting Details About an Account

Searching for Account Information

Searching for Account Information

You can display information about individual user accounts. The information includes viewing the highest permission path (the path the user accesses SQL Server through, either an administrator or user group) and viewing all permission paths for that user. You can also view SQL Server login IDs of users who exist in SQL Server but no longer exist in a Windows NT group that has access permission.

To search for account information

1. From the Security menu, choose Search.

   The Search for Account Information dialog box appears.

2. In the Account box, type the name of the user to search for information about.
3. Select the appropriate search:

   - To verify the highest permission path for the account, select the Verify Permissions for Account box.
   - To find all permission paths the account uses to access SQL Server, select Find All Permissions for Account box.

4. Choose the Search button.

   The results are displayed, including the full name of the account, the highest level permission the user has in SQL Server, and the permission paths the user is accessing SQL Server through.

5. To find SQL Server Login IDs without corresponding Windows NT accounts, select the Find Orphan SQL Login IDs box and then choose the Search button.

   If the search finds any SQL Server login IDs (other than sa and probe) that do not match Windows NT users with valid permissions, choose the Drop button to drop the SQL Server login IDs.

6. Choose the Cancel button.

Related Topic

Getting Details About an Account

Granting Privileges

Revoking Privileges

Getting Details About an Account

You can get details about a group or about a user within the group. For an individual user, you can add a login ID that matches the user's mapped username, or drop a matching login ID if it already exists. You can also add or drop a user from a database or set the default database. For a group account, the same actions apply to all members of the group. For example, you can update login IDs for a group, which will add login IDs that match the mapped usernames of the group's members, if the login ID does not already exist.

To view details about a user account

1. From the View menu, choose User Privilege.

   The groups with user privilege are displayed.
2. Double-click the group name that contains the user to get information about.

   The users within the group are displayed.
3. Select the user.
4. From the Security menu, choose Account Detail, or double-click the user name.

   The Account Detail dialog box appears. The Windows NT account name information for the user is displayed, as well as the user's mapped username.
5. Change any account information, as necessary.
6. Choose the Close button.

To view details about a group

1. From the View menu, choose User Privilege.

   The groups with user privilege are displayed.
2. Select the group.
3. From the Security menu, choose Account Detail, or press the CTRL key and double-click the group name.

   The Account Detail dialog box appears. The Windows NT account information for the group is displayed, as well as the group's mapped SQL Server name.
4. Change account information, as necessary.
5. Choose the Close button.

Related Topic

Searching for Account Information

Granting Privileges

Revoking Privileges

To connect to a SQL Server

1. In the Server box, select or type the name of a server.

   The Server box contains a list of the last 5 servers logged in to. To get a list of servers on the network, choose the List Servers button.
2. In the Login ID box, type your login ID. Then, in the Password box, type your password.

   Note that if you are using integrated security, you do not need to supply a login ID or password.
3. Choose the Connect button.

To connect to a server

1. In the Active Servers box, select the server.

   The Active Servers box lists the servers on the network. You can refresh the list by choosing the Refresh button.

2. Choose the OK button.

To configure SQL Security Manager

1. Set the appropriate configuration options.

- In the Login timeout box, type the amount of time, in seconds, that the server should wait before terminating a login attempt.
- In the Query timeout box, type the amount of time, in seconds, to wait, while retrieving query results.
- Select the ANSI->OEM box to activate the automatic ANSI to OEM conversion.

This activates character conversion to correct problems with extended characters displaying as graphics instead of letters with diacritical marks on Windows NT-based computers if SQL Server is not using the ANSI (ISO) character set. You must disconnect from SQL Server and reconnect for the selection to take effect. Be aware that this option affects all Windows- and Windows NT-based applications using the DB-Library API, not just SQL Security Manager (unless the DB-Library application explicitly overrides this setting).

- Select the Search for other permissions on drop box to specify that when you drop a login ID, all permission paths are searched and any other permission path the user or group is using to access SQL Server is dropped as well. Be aware that the search can take time.

2. Choose the OK button.

To set all options to their default values

- Choose the Defaults button.

To grant user privileges

1. In the Grant Privilege box, select the group that will have access to SQL Server.

   To show all local groups on the Windows NT-based computer, choose Local Groups. To show all groups on the default domain, select All Groups on the Domain.
2. The Add login IDs for individual group members is selected. This specifies that you want to create SQL Server login IDs for each user in the group.

   If you do not want each user in the group to have a separate SQL Server login ID, clear the check box. If you do not assign each user an individual login ID, the only way the user can access SQL Server is through the default login ID (usually "guest"). If you want to set up security like this, be sure that you've added a guest account when you set security options with the SQL Server setup program.
3. To add the users in the group to a database, so that database is their default database when they log in to SQL Server, select the Add Users to Databases box, and then select the database. It is recommended that you assign users to another default database instead of *master*, to discourage users from creating database objects in *master*. If you do not assign users to a default database, *master* becomes their default database.
4. Choose the Grant button.

To grant system administrator privilege

1. In the Grant Privilege box, select the group that will have access to SQL Server.

   To show all local groups on the Windows NT-based computer, choose Local NT Groups. To show all groups on the default domain, select All NT Groups on the Domain.

   Note that when you grant system administrator privilege, the Add Login IDs and Add Users to Database boxes are dimmed. This is because when you grant a group system administrator privilege to SQL Server, the users in the group are automatically mapped to the SA login ID and *master* is the default database.
2. Choose the Grant button.

To manage user Login IDs

The Windows NT account information for the user is displayed, as well as the user's mapped username.

1. If the user does not already have a matching login ID defined in SQL Server, the Add Login button is enabled. To add a login ID for this user, choose the Add Login button.
2. To allow SQL Security Manager to generate a random password for the user, the Generate Random Unique Passwords box is selected.

   If the user will be accessing SQL Server using both trusted and nontrusted connections, you may want to assign a known password instead. This password would be required for access through a nontrusted connection. To assign a known password, clear the Generate Random Unique Password box and type a password in the (Group) Password box.
3. You can also select a non-default language for the user, if multiple languages are installed on the SQL Server.
4. To remove the user's login ID from SQL Server, choose the Drop Login button. Note that if you have a default login created for the SQL Server, the user can still access SQL Server through the default login, unless you also remove the user from the Windows NT group.
5. Choose the Close button.

To manage users in databases

1. To add the user to a database, in the Available Databases box, select the database and then choose the Add User button. A group is created in the database with the same name as the Windows NT group at the top level of the tree (unless one already exists), and then the user is added to the database and group.
2. To set a database as the user's default database, select the database in the Databases Currently Defined In box, and then choose the Set Default button.
3. To remove a user from a database, select the database in the Databases currently defined in box, and then choose the Drop User button.
4. Choose the Close button.

To manage group login IDs

The Windows NT account information for the group is displayed, as well as the group's mapped username.

1. Choose the Update Logins button to add matching login IDs for all group members who do not already have one. This is necessary if you have added several new members to a Windows NT group that has user privilege to access SQL Server. Until the login IDs are updated, these new users can only access SQL Server using the default login ID.
2. To allow SQL Security Manager to generate a random password for the user(s) added when you choose the Update Logins button, the Generate Random Unique Passwords box is selected.

   If the user(s) will be accessing SQL Server using both trusted and nontrusted connections, you may want to assign a known password instead. This password would be required for access through a nontrusted connection. To assign a known password, clear the Generate Random Unique Password box and type a password in the (Group) Password box.
3. You can also select a default language for the user(s), if multiple languages are installed on the SQL Server.
4. To drop all login IDs for a group, choose the Drop All Logins button. Users in the group will then access SQL Server using the default login ID until the group privilege is revoked or you remove the users from the group in Windows NT (in which case the group still has access to SQL Server).
5. Choose the Close button.

To manage groups in databases

1. To update the database usernames for group members, select a database in the Available Databases

box, and then choose Update Users. If a group name matching the top-level Windows NT group name does not already exist, it will be created and all users will be added to it.

2. To drop a group's members from a database, select the database in the Available Databases box, and then choose Drop All Users. The group name will also be dropped from the database.
3. To set the default database for all members of the group, select the database in the Databases Currently Defined In box, and then choose the Set Default button.
4. Choose the Close button.

To revoke permission for a group

If you are viewing account details for a top-level group in the tree (one that has been granted user privilege), a Revoke button appears next to the account name. If you choose the Revoke button, all usernames will be dropped from all databases for the members of the group, all login IDs will be dropped, and user privilege will be revoked from the group.

To search for account information

1. In the Account box, type the name of the user to search for information about.
2. Select the appropriate search:
   - To verify the highest permission path for the account, select the Verify Permissions for Account box.
   - To find all permission paths the account uses to access SQL Server, select Find All Permissions for Account box.
3. Choose the Search button.

   The results are displayed, including the full name of the account, the highest level permission the user has in SQL Server, and the permission paths the user is accessing SQL Server through.
4. To find SQL Server login IDs without corresponding Windows NT accounts, select the Find Orphan SQL Login IDs box and then choose the Search button. If the search finds any SQL Server login IDs (other than sa and probe) that do not match Windows NT users with valid permissions, choose the Drop button to drop the SQL Server Login IDs.
5. Choose the Cancel button.

SQL Security Manager Keyboard Help

To get information about the keys for SQL Security Manager, choose from these topics:

SQL Security Manager Keys
Cursor Movement Keys
Dialog Box Keys
Menu Keys
Editing Keys
Help Key
System Keys
Text Selection Keys
Windows Keys

Editing Keys

Use the following keys to edit text:

Key(s)	Function
BACKSPACE	Deletes the character to the left of the insertion point, or deletes the selected text.
DEL	Deletes the character to the right of the insertion point, or deletes the selected text.
SHIFT+DEL	Deletes the selected text and places it on the Clipboard.
SHIFT+INS	Inserts text from the Clipboard to the active window.
CTRL+INS	Copies the selected text to the Clipboard.
ALT+BACKSPACE	Undoes the previous editing operation.

System Keys

The following keys can be used from any window, regardless of which application you are using:

Key(s)	Function
CTRL+ESC	Switches to the Task List.
Alt+ESC	Switches to the next application or minimized icon, including full-screen programs.
ALT+TAB	Cycles through running applications.
PRTSC	Copies an image of the entire screen contents to the Clipboard.
ALT+PRTSC	Copies an image of the SQL Security Manager window to the Clipboard.
ALT+F4	Closes the application.
CTRL+F4	Closes the active window.
F1	Displays Help information in SQL Security Manager dialog boxes.

Dialog Box Keys

Use the following keys within dialog boxes:

Key(s)	Function
TAB	Moves from option to option (left to right and top to bottom).

SHIFT+TAB	Moves from option to option in reverse order.
ALT+letter	Moves to the option or group whose underlined letter matches the one you press.
Arrow keys	Moves the selection cursor from option to option within a group of options. Or moves the cursor left, right, up, or down within a list or text box.
HOME	Moves to the first item or character in a list or text box.
END	Moves to the last item or character in a list or text box.
PAGE UP or PAGE DOWN	Scrolls up or down in a list box, one window at a time.
ALT+Up or Down arrow	Opens a drop-down list box and selects an item in a drop-down list box.
SPACEBAR	Selects or clears a check box.
SHIFT+Arrow key	Selects text in a text box.
SHIFT+HOME	Selects text from the cursor point to the first character in a text box.
SHIFT+END	Selects text from the cursor point to the last character in a text box.
ENTER	Executes a command button, or chooses the selected item in a list box and executes the command.
ESC or ALT+F4	Closes a dialog box without completing the command (same as the Cancel button).

Help Key

Use the following key to get Help information:

Key	Function
F1	Within a dialog box, pressing F1 displays the dialog box Help information. If the Help window is already open, pressing F1 displays information about how to use Help.

Cursor Movement Keys

Use the following keys to move the cursor (insertion point) in text boxes and other places where you can

type text:

Key(s)	Moves the insertion point
Up arrow	Up one line.
Down arrow	Down one line.
Right arrow	Right one character.
Left arrow	Left one character.
CTRL+Right arrow	Right one word.
CTRL+Left arrow	Left one word.
HOME	To the beginning of the line.
END	To the end of the line.
PAGE UP	Up one window.
PAGE DOWN	Down one window.
CTRL+HOME	To the beginning of the window or text area.
CTRL+END	To the end of the window or text area.

Text Selection Keys

Use the following keys to select text:

Key(s)	Function
SHIFT+Left or Right arrow	Selects text one character at a time to the left or right, or, if the character is already selected, cancels the selection.
SHIFT+Down or Up arrow	Selects one line of text up or down, or, if the line is already selected, cancels the selection.
SHIFT+PAGE UP	Selects text up one window, or, if the previous window is already selected, cancels the selection.
SHIFT+PAGE DOWN	Selects text down one window, or, if the next window is already selected, cancels the selection.
SHIFT+HOME	Selects text to the beginning of the line.
SHIFT+END	Selects text to the end of the line.
CTRL+SHIFT+Left arrow	Selects the previous word.
CTRL+SHIFT+Right arrow	Selects the next word.
CTRL+SHIFT+HOME	Selects text to the beginning of the document.
CTRL+SHIFT+END	Selects text to the end of the document.

Menu Keys

Use the following keys to select menus and to choose commands:

Key(s)	Function
ALT or F10	Selects the leftmost menu on the menu bar.
ALT + letter	Chooses the menu or menu item whose underlined letter matches the one you press.
Left or Right arrow	Moves among menus.
Up or Down arrow	Moves among menu items.
ENTER	Chooses the selected menu item.
ESC	Cancels the selected menu.

Windows Keys

Use the following keys to navigate in the Microsoft Windows or Windows NT operating systems:

Key(s)	Function
ALT+SPACEBAR	Opens the System menu for an application.
ALT+- (Hyphen)	Opens the System menu for a document window.
ALT+F4	Closes an application.
ALT+ESC	Switches to the next application or minimized icon, including full-screen programs.
ALT+TAB	Cycles through running applications.
ALT+ENTER	Switches an application for an operating system other than Windows between running in a window and running full screen.
Direction keys	Moves a window when you have chosen Move from the System menu, or changes the size of a window when you have chosen Size from the System menu.

SQL Security Manager Keys

The following keys are specific to SQL Security Manager when you are viewing an outline of the users or groups:

Key(s)	Function
CTRL+N	Displays the Connect Server dialog box.
ENTER	Expands or collapses a group or shows account detail for a user.
ESC	Cancels the enumeration of groups in the outline tree.
CTRL+ENTER	Shows account detail for a group.
UP ARROW	Moves up one item in the visible outline tree.
DOWN ARROW	Moves down one item in the visible outline tree.
PAGE UP	Scrolls up one window in the visible outline tree.
PAGE DOWN	Scrolls down one window in the visible outline tree.