

UC for Business - Security



Table of Contents

Introduction.....	3
Overview.....	3
Features	3
Benefits	4
Securing Functions	4
Administrator Functions	4
Centralized Preferences	4
Individual User Functions.....	5
Operator Functions.....	5
Mailbox Functions	5
Securing Objects.....	5
Objects and Actions	5
Object Example.....	6
Action Example.....	6
Creating Security Classes	6
What is a Security Class?.....	6
What is a Pre-Defined Role?	6
Allocating Users to Security Classes.....	7

Introduction

In today's business environment, protecting applications against unauthorized use is a priority. The security features of NEC's UC for Business (UCB) tailor access to system applications and functionality to meet an organization's specific requirements.

Whether an organization has high inter-departmental security requirements, operates in a multi-tenanted environment or simply wants to control costs, NEC's UC for Business has the security features to meet all current and future needs.

Overview

UC for Business Security offers a comprehensive set of security features for organizations that require inter-departmental security restrictions or operate in a multi-company tenanted environment. These features are included as part of CT Control and allow companies to restrict viewing and editing rights to protect individual set-up and operating parameters.

Security features can also be used to control costs, as they allow organizations to restrict access to specific functionality, such as transferring from a user's voice message greeting to their mobile telephone. Access to functions and fields within the software can be defined for every person using general security class permissions and/or individual user permissions.

Depending on the security level set for security classes and/or an individual user, users may, for example, be permitted/restricted access to the following:

- Viewing configuration screens in Administrator
- Viewing configuration screens in other UCB applications such as Agent Desktop, Voice Messaging and Reports set-up
- Viewing specific options, such as toolbar buttons, in UCB applications
- Making changes to the configuration of the system using Administrator
- Making changes to settings for other UCB applications such as Agent Desktop and Reports
- Hearing certain menu options in Voice Messaging
- Sending voice messages to specific mailboxes
- Setting up one-touch mailbox options that perform transfers to external telephone numbers

- Sending messages to certain mailboxes when using the Name Search functionality from within a mailbox
- Dialing certain extensions when using the Dial by Name search from the auto attendant
- Monitoring phone inbound or outbound calls (Queued or direct)

The security settings are implemented using four key parameters:

- **Security classes** - Each user belongs to a Security Class which contains certain permissions and restrictions. When a user is required to have permissions in addition to those set for their class, these permissions can be enabled specifically for that user.
- **Function-based control** - This is used to restrict the main functions a user can perform within each module. Examples are: use Administrator; edit Companies, Holidays, Security settings; remember PIN; Record conversations; Record name; and Edit personal distribution lists.
- **Object-based access control** - An "object" is something administrators, supervisors and agents "can do something to." Some examples of objects are: queues, mailboxes, agents, lines (extensions) and wallboards. The system administrator can control what type of access an individual user and/or a security class has to these objects by. Access may be 'None,' 'View only' or 'Edit.'
- **Company/Department** - Multiple companies and departments can be configured with their own operating parameters and security permissions within a single UCB site.

Once these four parameters are set, they can be modified by the system administrator using a simple graphical interface.

Features

UCB offers a comprehensive set of security features:

- Every user is assigned to a security class based on their role within the organization.
- There is no system limit to the number of security classes that can be configured.
- Hundreds of different functions within the system can be restricted and controlled using the security features.
- If changes are made to a security class, those changes will be applied to all users assigned to that security class the next time they log in.
- Changes can be made to a single user within a security class without affecting the security settings of any other user in that security class.
- The system remembers an individual's unique security settings within a security class and does not allow future changes to a security class to override those settings.

- To simplify the task of configuring security settings, default security roles can be used as the basis for a security class. These default roles include system administrator, company administrator, queuing supervisor, agent, voice messaging user and console operator.
- Icons within Administrator visually illustrate the level of security access an individual user or security class has to a particular function within the system. For example, a 'pencil' icon next to an Administrative function denotes the security access level on this function is 'Edit.' An 'eye' icon would denote the security access level on this function is 'View Only.'

Benefits

Whether security requirements are complex or simple, the security features of UCB offer significant benefits:

- Security classes can be tailored to most roles in a company giving organizations the flexibility to co-exist in multi-company or multi-departmental environments, while being assured application configurations and reports of each company or department are secure.
- Businesses can control costs by restricting specific features, such as one-touch options from Voice Messaging which allow callers to transfer to external telephone numbers.
- Once created, security classes can be allocated to multiple users, eliminating the need to create a security profile for every individual user. This significantly reduces the amount of system administration required without compromising on the level of security across the organization.
- Pre-defined roles and default security settings further minimize the amount of system administration required.
- Flexibility to change security settings on an individual basis where required.
- Security icons give the system administrator an immediate view of what settings and access rights have been assigned to each security class and individual. This makes the task of creating and editing security classes that much simpler.

Securing Functions

The security functionality of UCB allows organizations to control access to functions and objects within the system.

Within each securityClass administrative and operational access can be restricted at the highest level to each of the applications, such as Administrator, Desktop, Console, Voice Messaging and Application Manager.

Within each of these applications, access to specific functions can be permitted or denied by simply ticking the relevant boxes. The following is an overview of the functions that can be secured within each module. For a more detailed look at each module's functionality, please refer to the relevant white paper.

Administrator Functions

Typically, only a few users at a UCB site require access to the Administrator application. Using UCB, provision can be made for administrators requiring different levels of access, for instance an overall site administrator may have access to full functionality, including:

- Edit security settings for own company
- Edit security settings for all companies
- Edit companies
- Control client applications
- Control server applications
- View ports status
- Administer remote sites

A contact center or departmental administrator may only require these functions:

- Run queuing wizard to add new queues
- Run voice messaging wizard to add new mailboxes
- Use copy manager to copy existing queue functionality from one queue to another
- Edit Query database
- Edit holidays
- Run reports
- Use Audit Trail report
- Change queue modes

The operator may be provided with access to useful office administration functions directly from Console:

- Add/Edit global Presence (Speed-dial) pages
- Edit global Phonebook (office and customer directory)

Centralized Preferences

Administrators can edit, copy, import and export user preferences for Desktop, Console and Executive Insight from a single location in the Administrator application. The following functions are available:

- Edit User Preferences for multiple users at one time, for example, assign the same preferences to all users with a certain security class.

- Restrict the ability of individual users to edit their User Preferences via Desktop, Console or Executive Insight.
- Copy User Preferences from one user to other users.
- Export User Preferences to a text file for future use.
- Import preferences from a previously saved text file.

Individual User Functions

Users can be restricted from the highest level of operability, assisting managers to manage application licenses. The following restrictions are available per user, preventing them from:

- Running Desktop as an Agent
- Running Desktop as a Voice Messaging user
- Running Console
- In some businesses, managers may wish to restrict configuration access for individual Desktop users, for example to prevent them from altering a global office configuration template. Restricted access may include these functions:
 - + Add personal Presence pages
 - + Remember PIN number (PIN is automatically populated; while many users value this option, managers in a high-security environment won't want them using it)
 - + Use Microsoft Windows® Logon (allows users to run Desktop automatically on Windows® startup)
 - + Change recall timers for held or transferred calls
 - + View recent calls panel
 - + Integrate with Microsoft Outlook® contacts

User operation can also be restricted with Security, for example certain users may be prevented from using the following functionality:

- Pick up calls remotely from other extensions
- Send messages to Digital phone (may annoy other users)
- Record conversations (a valuable feature, but one that may put a load on resources if abused)
- Use Web Browser
- Make internal Chat calls (between Desktop and Console users)
- Select media types to log into
- Skip ETR (forces users to enter an Expected Time of Return)

Agent-specific restrictions in Desktop include:

- Change default Worktime
- Select queues to view

- Select classes to view
- Transfer Chat calls
- Break configuration

Operator Functions

Console users can be empowered with or denied significant Console-specific functionality:

- Login/Logout
- Break configuration
- Change recall timer on held or transferred calls
- Change ring tones for incoming calls based on called number
- View calls parked for another company

Mailbox Functions

Mailbox users can be prevented from recording their own mailbox names or greetings or configuring their own:

- Caller Profiles
- Distributions lists
- Schedule
- Advanced Options
- One-touch keys
- Notification

Access to specific Mailbox One-Touch Key functions such as Select 'Direct Dial' option or Select 'Transfer' options can also be restricted.

Securing Objects

Objects and Actions

At the lowest level, access to specific 'objects' within the system can also be restricted. These are examples of objects which can be restricted:

- Queues
- Agent Login Classes
- Users
- Agents
- Mailboxes
- Mailbox Classes
- Distribution Lists

- System Queues
- Patterns
- Lines
- Phonebook Directories
- Wallboards
- Wrapup Templates
- Totaling Queues
- Groups
- Voice Prompts
- Alerts

Object Example

Access to selected items in an object group can be blocked or moderated. For example, there may be three specific queues in the Queues object group: Sales, Customer Service and Accounts. Use Security to ensure only users from the Sales department interact with the Sales queue, and so on. Possible interactions would include configuring, viewing or taking calls from the queue.

Action Example

For each object there are a number of actions or interactions which can be restricted.

For example, the following permissions can be permitted or denied for 'Queues':

- View Queues
- Edit Queues
- Change Modes of the Queues
- View Alerts for these Queues
- Edit Queue Modes
- Transfer Calls to Chat Queues
- Make Internal Calls to Chat Queues

Creating Security Classes

What is a Security Class?

The system administrator can configure a group of users with similar access requirements, without needing to set up individual specifications.

Often, however, one user with 99% of the same requirements as the rest of the group also needs access to just one extra function. UCB can accommodate this need by allowing an individual's requirements to be customized while still remaining part of the class. This saves the site from the maintenance nightmare of having as many classes as there are users, each needing separate attention whenever a change is requested.

Wizards make it easy to create a new security class. The 'Add' wizard template prompts the system administrator to enter the required information, such as:

- Company and department the security class will apply to
- Class name, for example, "Voice Messaging User," a wide security class encompassing all staff with voice mailboxes
- Whether the class is to be based on a pre-defined role or an existing class setup

The wizard assists system administrators in configuring new classes by allowing them choose a 'pre-defined role' from a pre-configured list in the system, or to 'use settings from an existing security class.'

What is a Pre-Defined Role?

A pre-defined role assists the administrator in setting the authorization for each security class. A class can be based on more than one pre-defined role if, for example, the class will contain people who are agents as well as voice messaging users. Examples of pre-defined or default roles are:

- The System Administrator role has full access to all objects in the system.
- The Company Administrator role has full access to all objects belonging to a selected company.
- The Queuing Supervisor role has permission to run Desktop and access the Queuing features of the application as well as edit queuing objects and remotely change agents' states.
- The Agent role has permission to run Desktop and access the basic Queuing features of the application.
- The Voice Messaging User role has permission to run Desktop and access the Voice Messaging features of the application.
- The Console Operator role has permission to run Console and make changes to the Phonebook and global Presence or Speed-dial pages.

Allocating Users to Security Classes



Figure 1. Creating a new Security Class with the Wizard, using Pre-defined roles

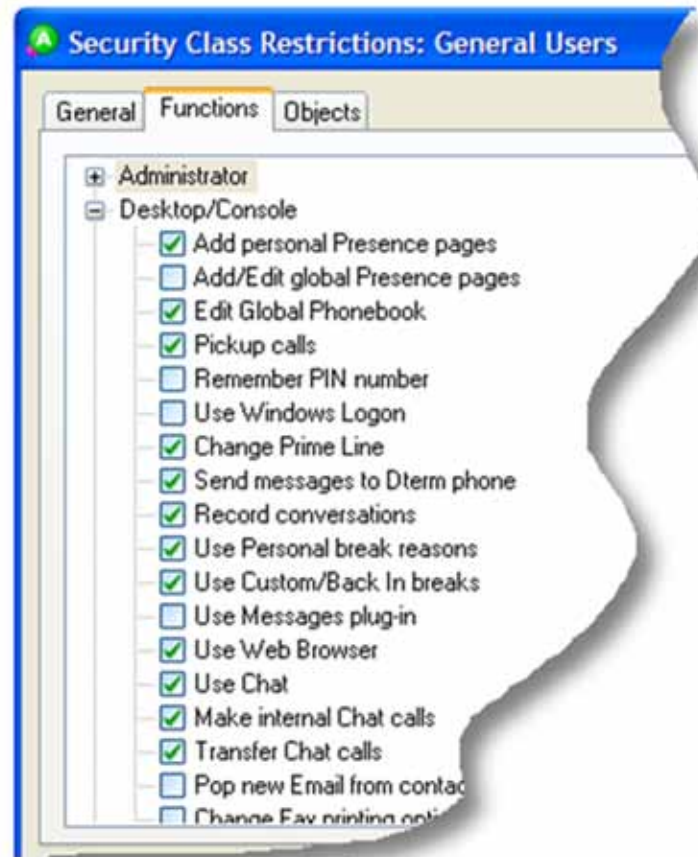


Figure 2. Customizing Security options for a Class (or individual)

For more information, visit www.nec.com.au, email contactus@nec.com.au or call 131 632

Oceania (Australia)
NEC Australia Pty Ltd
www.nec.com.au

Corporate Headquarters (Japan)
NEC Corporation
www.nec.com

North America (USA)
NEC Unified Solutions Inc.
www.necunifiedsolutions.com

Asia
NEC Corporation
www.nec.com

Europe (EMEA)
NEC Unified Solutions
www.nec-unified.com

About NEC Australia Pty Ltd. NEC Australia is a leading supplier and integrator of ICT solutions to carriers, government and businesses. Through a national network of engineering and support staff backed by over 200 partner organisations, we design, develop and deploy advanced IT/Network communication solutions and services using best-of-breed technologies in multi-vendor environments. Our business encompasses Hosted Application and Network Services, Systems Integration, IP Communications Servers, PBX, Broadband Access Systems, Data Centre and Cloud Technology Services along with Digital Signage and Displays.

UCB_S_WP | v2 28.10.10

NEC Australia Pty Ltd reserves the right to change product specifications, functions, or features, at any time, without notice. Please refer to your local NEC representatives for further details. Although all efforts have been made to ensure that the contents are correct, NEC shall not be liable for any direct, indirect, consequential or incidental damages resulting from the use of the equipment, manual or any related materials. The information contained herein is the property of NEC Australia Pty Ltd and shall not be reproduced without prior written approval from NEC Australia Pty Ltd.

Copyright © 2010 NEC Australia Pty Ltd. All rights reserved. NEC, NEC logo, and UNIVERGE are trademarks or registered trademarks of NEC Corporation that may be registered in Japan and other jurisdictions. All other trademarks are the property of their respective owners. All rights reserved. Printed in Australia. Note: This disclaimer also applies to all related documents previously published.