Best Practices guide to security settings in Service Manager

When to use Profile security, Mandanten security, or Security Folders.

HP® Software — Service Management

Introduction

Restricting user's access to data is a common concern in enterprise applications. Service Manager offers several ways of restricting user access to its data. The restrictions can be on offering users only certain forms to view their data, or offering only a certain set of options for actions on the record, as well as limiting the records returned on a query against the database. This document will discuss these different ways, their pros and cons, and recommended use.

Requirements

Administrator access to Service Manager 7.00 or higher is required to set these security features.

Security Features

There are three different ways in which data access can be limited in Service Manager:

1. By limiting the form used to display data based on the user's role:

   Use Forms Designer to create a form displaying only the data that is relevant for the user. Then assign this form to the user in the profiles, or in links, or based on his capabilities via the initialization Process.
2. By limiting the options the user has on the record

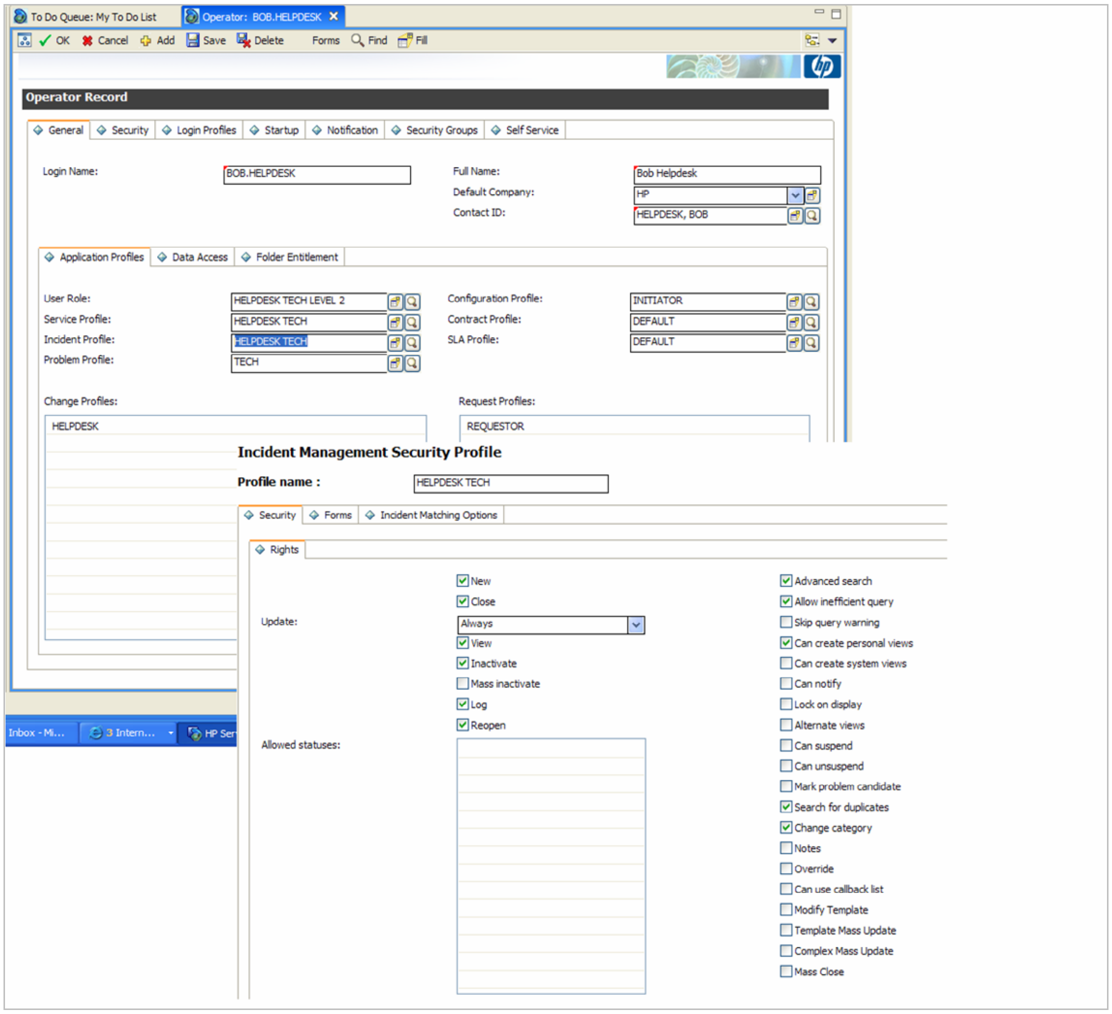
   Limiting options can be done based on profiles, format control privileges or capability words. Profiles and capability words are assigned to the user in the operator record, format control privileges are assigned to the form or table.
3. By limiting the records returned from the database

   Limiting the records returned from the database is usually done with the Mandanten feature. It is also possible to append to a user's query via the profile's append.query field.

Note: Capability words and Forms are not security features per se, but can be used as helpers to determine to which data and options the user has access.

Module Profiles

Profile controls are available for all modules – with the exception of Service Catalog. Module profiles are assigned to the user in the operator record and are the same for every record for that module. They define in detail if the user can perform actions such as view, create, update, or close records in the tables for this module. The profile application defined in the Object record determines the appropriate rights for that table. The profile rights are set on the RAD level and typically determine if a display option (button) is available to the user.



Operator Record

Login Name: BOB.HELPDESK

Full Name: Bob Helpdesk

Default Company: HP

Contact ID: HELPDESK, BOB

User Role: HELPDESK TECH LEVEL 2

Service Profile: HELPDESK TECH

Incident Profile: HELPDESK TECH

Problem Profile: TECH

Configuration Profile: INITIATOR

Contract Profile: DEFAULT

SLA Profile: DEFAULT

Change Profiles: HELPDESK

Request Profiles: REQUESTOR

Incident Management Security Profile

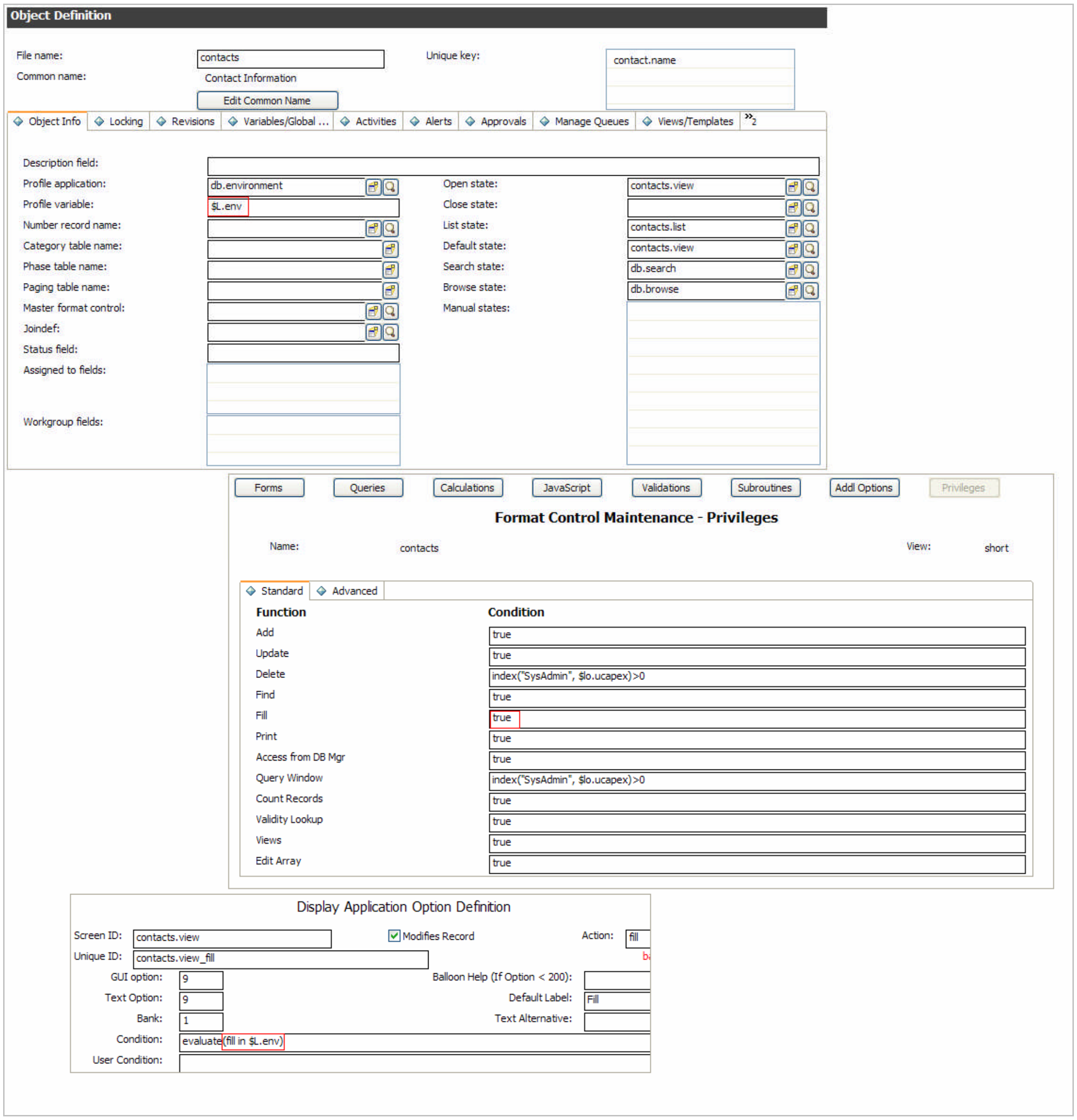
Profile name : HELPDESK TECH

☑ New
☑ Close
Update: Always
☑ View
☑ Inactivate
☐ Mass inactivate
☑ Log
☑ Reopen
Allowed statuses:

☑ Advanced search
☑ Allow inefficient query
☐ Skip query warning
☑ Can create personal views
☐ Can create system views
☐ Can notify
☐ Lock on display
☐ Alternate views
☐ Can suspend
☐ Can unsuspend
☐ Mark problem candidate
☑ Search for duplicates
☑ Change category
☐ Notes
☐ Override
☐ Can use callback list
☐ Modify Template
☐ Template Mass Update
☐ Complex Mass Update
☐ Mass Close

Format Control Privileges

Format Control privileges are used for all tables that are not protected by module profiles, such as the contacts or operator tables, or when accessing tables in Administrative Mode from Database Manager. The profile application db.environment defined in the Object record determines the appropriate rights based on Format Control privileges. The Format Control privileges are set on the RAD level and usually determine whether a button (display option) is available to the user. Format Control privileges of the master format control typically apply to all records in the table, whereas privileges of a detail Format Control apply to all records viewed from that specific form.



Object Definition

File name: contacts

Common name: Contact Information

Unique key: contact.name

Description field:

Profile application: db.environment

Profile variable: $L.env

Number record name:

Category table name:

Phase table name:

Paging table name:

Master format control:

Joindef:

Status field:

Assigned to fields:

Workgroup fields:

Open state: contacts.view

Close state:

List state: contacts.list

Default state: contacts.view

Search state: db.search

Browse state: db.browse

Manual states:

Format Control Maintenance - Privileges

Name: contacts

View: short

Function	Condition
Add	true
Update	true
Delete	index("SysAdmin", $lo.ucapex)>0
Find	true
Fill	true
Print	true
Access from DB Mgr	true
Query Window	index("SysAdmin", $lo.ucapex)>0
Count Records	true
Validity Lookup	true
Views	true
Edit Array	true

Display Application Option Definition

Screen ID: contacts.view

☑ Modifies Record

Action: fill

Unique ID: contacts.view_fill

GUI option: 9

Balloon Help (If Option < 200):

Text Option: 9

Default Label: Fill

Bank: 1

Text Alternative:

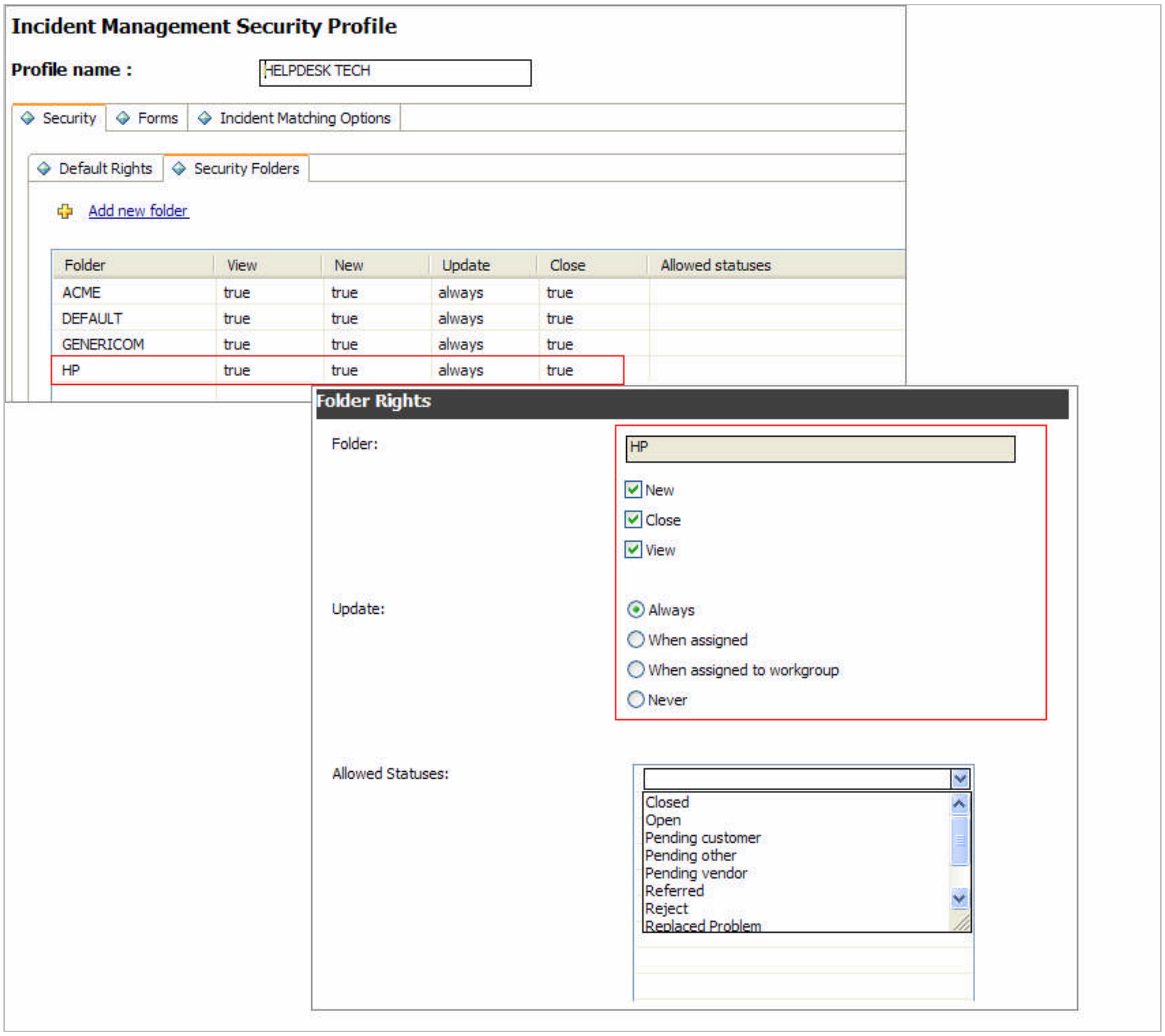
Condition: evaluate(fill in $L.env)

User Condition:

Security Folders

Security Folders can be used to set user rights, such as create, update, or close on a record by record basis. Which rights are applied is determined based on the content of the folder field of the specific record. Security Folders combine benefits of Mandanten Security in that a subset of records can be restricted as well as Module Profiles in that the restrictions are to the view / create / update level.

Security Folders are globally enabled or disabled in the System Information Record and implemented on the application level. Available folders are defined in the FolderDef table. Security Folder rights are assigned to the operator via the module profile and are only available where module profiles are available. Each operator may have a default folder assigned in the operator record that is used for filling in the folder value on every ticket this operator creates.



Incident Management Security Profile

Profile name : HELPDESK TECH

Folder	View	New	Update	Close	Allowed statuses
ACME	true	true	always	true	
DEFAULT	true	true	always	true	
GENERICOM	true	true	always	true	
HP	true	true	always	true	

Folder Rights

Folder: HP

☑ New
☑ Close
☑ View

Update:
● Always
○ When assigned
○ When assigned to workgroup
○ Never

Allowed Statuses:
Closed
Open
Pending customer
Pending other
Pending vendor
Referred
Reject
Replaced Problem

Note: If security folders are used, every profile has to have a setting for every possible folder value. If a folder value is missing, the user will not be able to view records in this folder.

Mandanten Security

Mandanten security is typically used in a Multi-Service Provider (MSP) environment. It is available for all tables in Service Manager.

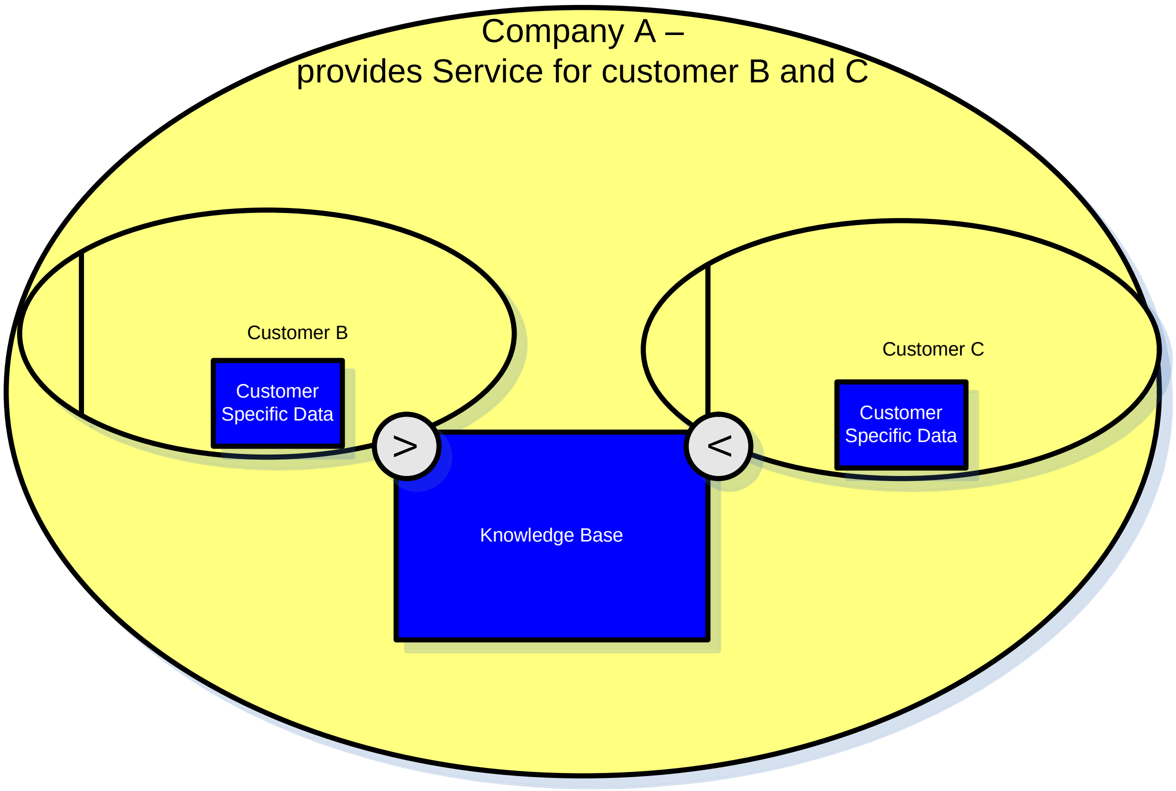
Mandanten security is implemented in the RTE layer where a limiting query is automatically added to queries issued against any protected table. Due to this implementation a user either has access to a record or not.

Mandanten Security is set up via the operator record, where the operator can belong to none, one or many security groups. The security groups define which values in the Mandanten field make the record visible or invisible. The Mandanten field for the protected table is defined in the scmandant table.

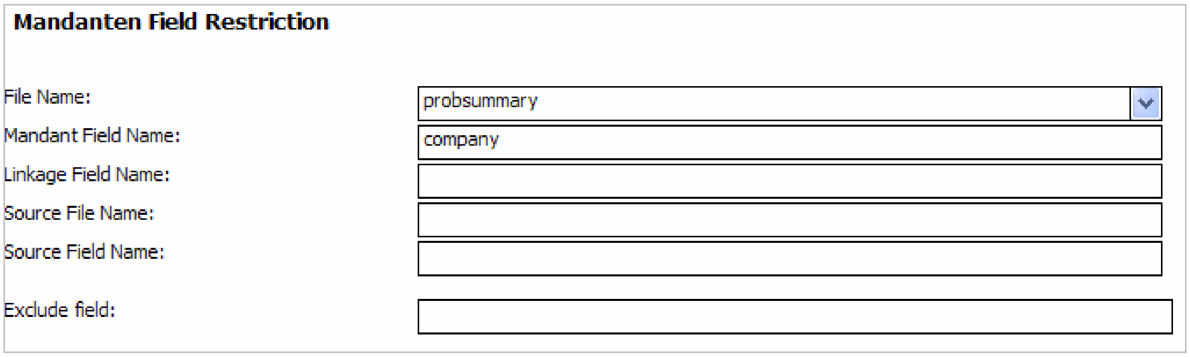
Note: When Mandanten-protecting related tables, make sure to have the related value visible, for example, if you are allowed to see records of category *Hardware*, ensure that the Hardware category record is visible as well.

Example:

Company A provides service for customers B and C. Customers B and C do not want to share any incident data, but want to share knowledge in the KB table.



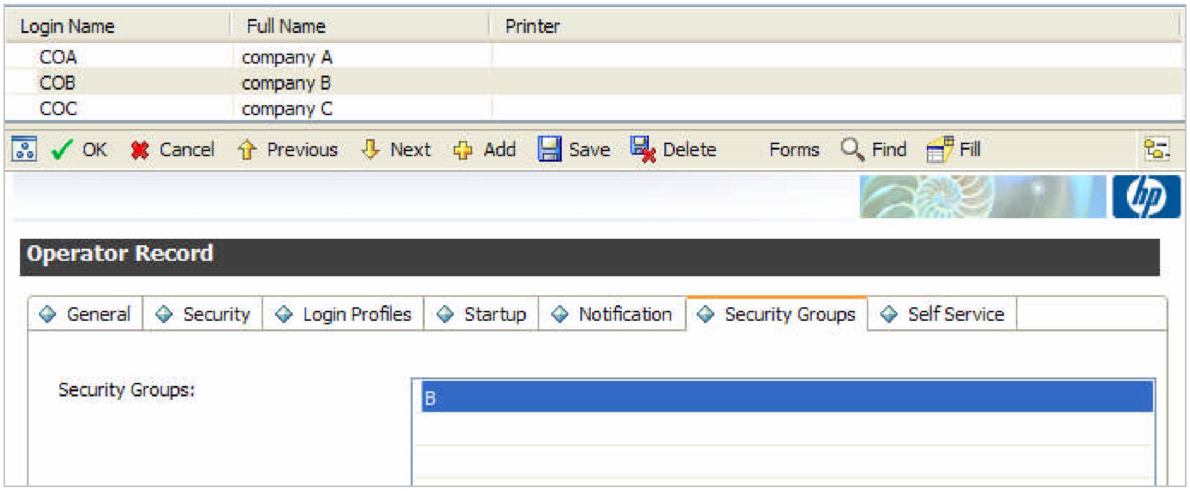
The Mandanten field would be the company field in the Incident Management tables. The Knowledge Base table will not be protected, since it is shared between all companies, so no scmandant record should be created against that table.



Mandanten Field Restriction

File Name:	probsummary
Mandant Field Name:	company
Linkage Field Name:	
Source File Name:	
Source Field Name:	
Exclude field:	

The security groups for operators would be B for employees of customer B, C for employees of customer C, and A for employees of company A.

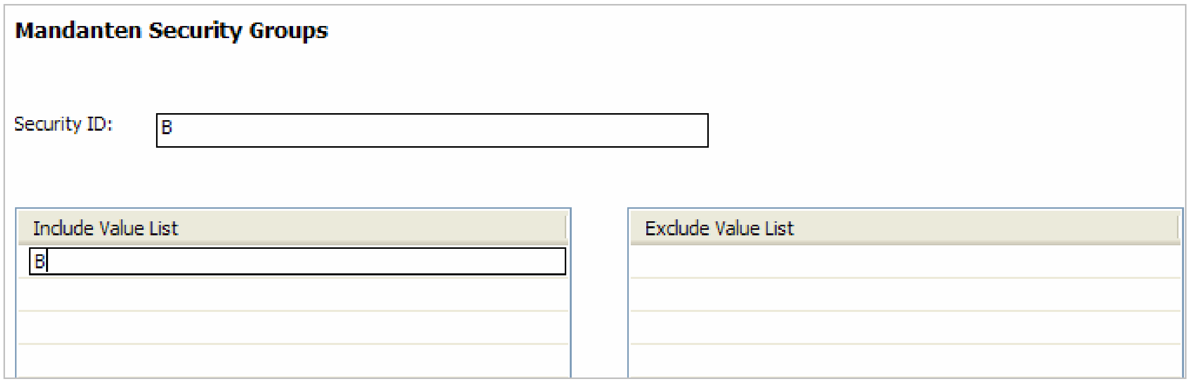


Login Name	Full Name	Printer
COA	company A	
COB	company B	
COC	company C	

Operator Record

Security Groups: B

The allowed values (include list) for customer B is B, for customer C is C and for company A is A, B, C (since they are servicing all customers).



Mandanten Security Groups

Security ID: B

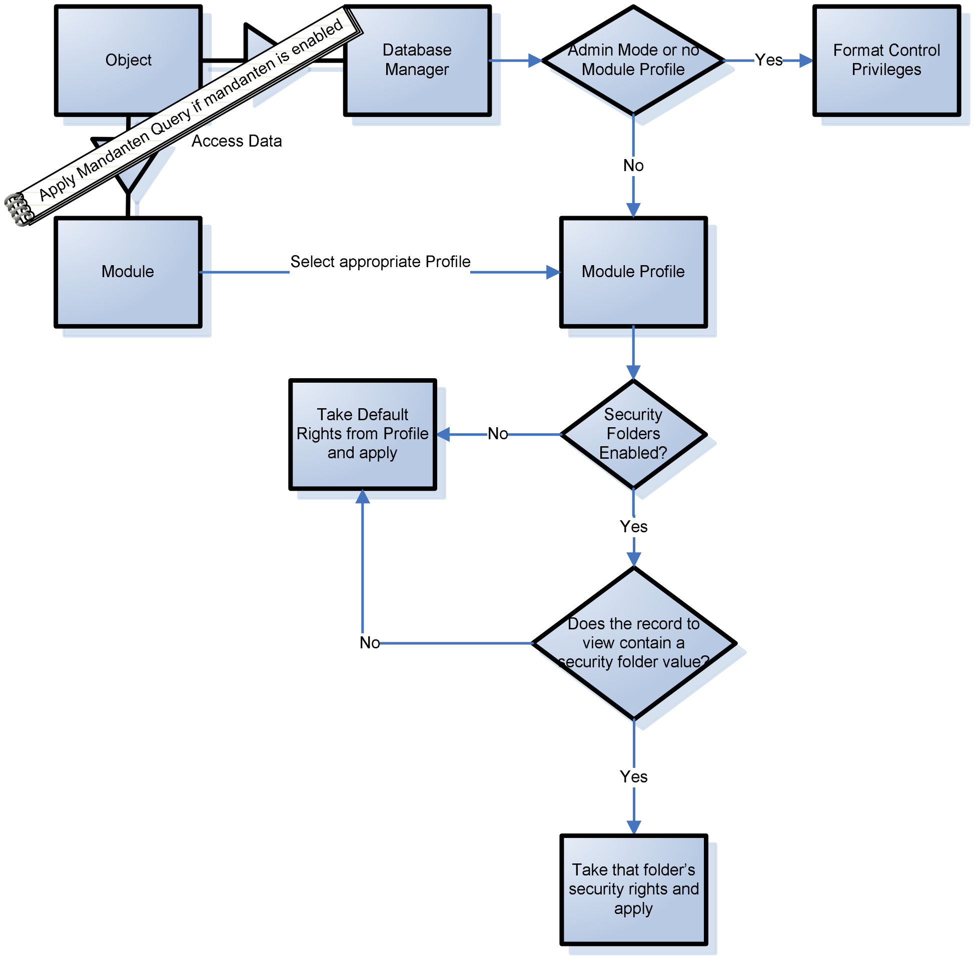
Include Value List	Exclude Value List
B	

Best Practices: What to use when

Each of the previously described security concepts has different areas of use. Format Control Privileges and Module Profile rights are always set up. Security Folders and Mandanten protection are additional features that typically are used in MSP implementations.

Security Feature	Available on all Tables	Optional / Mandatory	Implemented on … layer	Typically used by MSPs
Module Profiles		Mandatory	Application	
Format Control Privileges	X	Mandatory	Application	
Security Folders		Optional	Application	X
Mandanten	X	Optional	RTE	X

Precedence workflows


Object
Apply Mandanten Query if mandanten is enabled
Database Manager
Admin Mode or no Module Profile
Yes
Format Control Privileges
Access Data
No
Module
Select appropriate Profile
Module Profile
Take Default Rights from Profile and apply
No
Security Folders Enabled?
Yes
No
Does the record to view contain a security folder value?
Yes
Take that folder's security rights and apply

Note: Mandanten restrictions are in addition to any other restrictions and are added on the binary level by modifying the query issued to the database.

Security Features for general use

Module Profiles and Format Control Privileges are complementary – Format Control Privileges are used to determine user rights if no Module Profile controls this table, or when viewing the data via Database Manager in Administration Mode. The profile application in the Object record determines which control is used –db.environment utilizes the Format Control settings whereas applications such as im.environment (for Incident Management), cc.environment (for Service Desk), or cm.environment (for Change Management) use the Module Profile settings.

The Security Folder settings are determined by the user's Profile. They override the Module Profile settings if Security Folders are enabled and the record to view contains a folder value.

Security Feature	**Protection Level**	**Protection Detail**
Format Control Privileges	Table / Form	Create, update, close, delete
Module Profiles	Table	Create, update, view, close
Security Folders	Folder Field (typically Company)	Create, update, view, close
Mandanten	Mandant Field (typically Company)	Visible or Not

Security Features typically used at an MSP

Both Mandanten and Security Folders are typically used in a Managed Service Provider (MSP) environment. The determining factor is the granularity of access: Should the customers in the MSP environment be able to view certain data with limited rights or should they not be able to view the data at all. If the data is supposed to be completely segregated, then Mandanten is the concept to implement. If the data access is supposed to be limited, but not completely taken away, Security Folders work best.

In Security Folders, you can give certain rights based on the folder value, which typically is the name of the MSP customer. These rights are:

- Create
- Update
    - Update only under certain circumstances
- Close
- View
- Update access to records in a certain status

Both concepts may be used in the same system on different tables. For example the operator table may be Mandanten protected, whereas probsummary data can be viewed by all parties and only modified by a certain group.

Security Folders can mimic Mandanten- behavior by removing all rights for a certain folder, or not including a folder in the list of a profile's folder accesses. Mandanten protection would be more efficient in this case though, since it modifies the query that retrieves the records, rather than determining on a record by record basis if this record can be viewed.

For more information

Please visit the HP Software support Web site at:

www.hp.com/go/hpsoftwaresupport

This Web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued customer, you can benefit by being able to:

- Search for knowledge documents of interest
- Submit and track progress on support cases
- Submit enhancement requests online
- Download software patches
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter discussions with other software customers
- Research and register for software training

Note: Most of the support areas require that you register as an HP Passport user and sign in. Many also require an active support contract.

To find more information about support access levels, go to the following URL:

www.hp.com/go/hpsoftwaresupport/new_access_levels

To register for an HP Passport ID, go to the following URL:

www.hp.com/go/hpsoftwaresupport/passport-registration

06/2007