Progress®

# The 5 W's of Dynamic Data Masking

## Progress OpenEdge Dynamic Data Masking: Managing Data Privileges

**Sunil Jardosh**
Progress, Burlington, USA
sjardosh@progress.com

# Agenda

- Business Needs
- What is DDM?
- Preparing to Roll Out DDM
- Configuring DDM in OpenEdge 12.8
- Demo
- Resources
- Q&A

© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

All roadmaps are for informational purposes only, and the reader is hereby cautioned that actual product development may vary significantly from roadmaps.

These roadmaps may not be interpreted as any commitment on behalf of Progress, and future development, timing and release of any features or functionality described in the roadmaps remains at our sole discretion.

Progress®

© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

Organizations must strive to meet **regulations** regarding data security and permissions **to help prevent sensitive information** like payment card information from being **viewed by unauthorized users**.

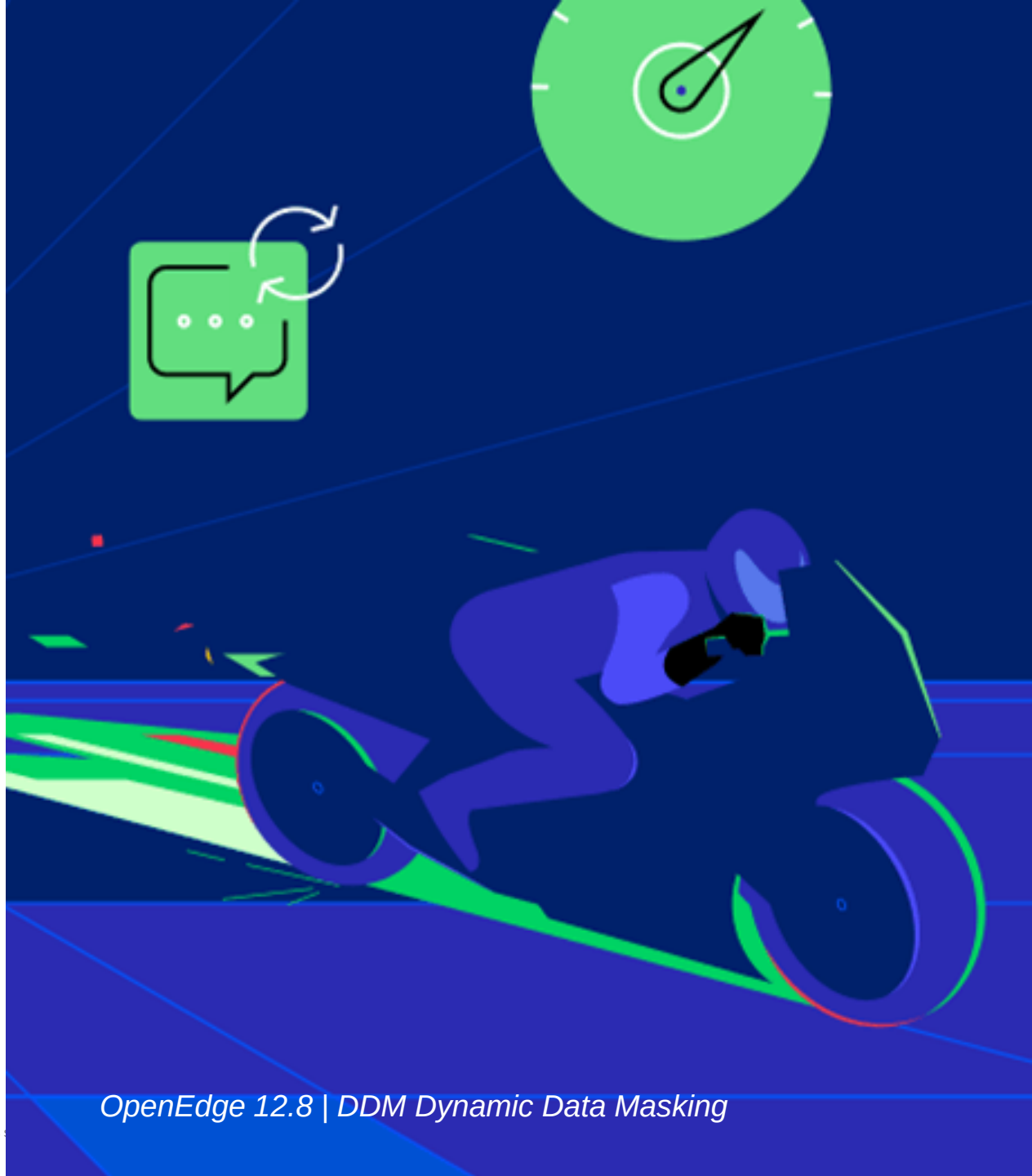
- No changes to the application code
- No changes to underlying data
- Configuration based
- High performance, high availability

**Authorized**

| First Name | Last Name | CC Information |
|---|---|---|
| Liam | Smith | 4532 1234 5678 9012 |
| Noah | Jones | 6011 2345 6789 0123 |
| Emma | Brown | 5100 9876 5432 1098 |
| Olivia | Johnson | 3712 3456 7890 1234 |

**Unauthorized**

| First Name | Last Name | CC Information |
|---|---|---|
| Liam | Smith | xxxxxxxxxxxxx9012 |
| Noah | Jones | xxxxxxxxxxxxx0123 |
| Emma | Brown | xxxxxxxxxxxxx1098 |
| Olivia | Johnson | xxxxxxxxxxxxx1234 |





© 2024 Progress Software Corporation and/or its

# What is DDM?

© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

# OpenEdge 12.8: Dynamic Data Masking

- Helps you meet data privacy and integrity compliance requirements such as GDPR, HIPAA and PIPEDA
  - A compliance feature for helping to obscure personally identifiable information (PII)
- Part of Progress Advanced Security Package





© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

# OpenEdge 12.8: Dynamic Data Masking (Cont.)

- Field level, closed access model
  - Masked field, by default, gets masked data
- Role-Based Access Control (RBAC)
  - Roles/Privileges granted to the user to unmask the data

| First Name | Last Name | CC Information |
|---|---|---|
| Liam | Smith | XXXXXXXXXXXX9012 |
| Noah | Jones | XXXXXXXXXXXX0123 |
| Emma | Brown | XXXXXXXXXXXX1098 |
| Olivia | Johnson | XXXXXXXXXXXX1234 |

© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

# Preparing to Roll Out DDM

Progress®

© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

- WHAT: Sensitive information/fields
- WHO: Is allowed to have access
- Application: Employee Information System
  - Single user interface for all users
  - Obscure sensitive information based on user login

Protected

Private

| | HR Manager | HR | Manager | Rest of all |
|---|---|---|---|---|
| Contact info | View | View | View | View |
| Leaves | View | View | View | Mask |
| Benefits | View | Mask | View | Mask |
| SSN | View | Mask | Mask | Mask |

© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

# Terminology for DDM

© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

# Terminology for DDM

## Mask

- How to hide the data from unauthorized users?
- Field-level configuration
- Masked value is field type compatible

| | |
|---|---|
| **Partial** | **P: prefix,char[:maxchars][,suffix]**<br>my@email.com => P:1,*:4,4<br>m****.com<br>4532 1234 5678 9012=>P:0,X,4<br>XXXXXXXXXXXX9012 |
| **Null** | Displays NULL, **N:** |
| **Literal** | Display Literal **L: Literal Value** |
| **Default** | Display default mask Value **D:** |

| First Name | Last Name | CC Information |
|---|---|---|
| Liam | Smith | 4532 1234 5678 9012 |

| First Name | Last Name | CC Information |
|---|---|---|
| Liam | Smith | XXXXXXXXXXXX9012 |


© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

# Masking Types

Default: `XXXX` Lift Tours

*Replaces whole field value with X's*

Partial: `(617) 450-0086` `XXXXXXXXXX0086`

*Replaces a specified part of the value with X's*

Literal: `Burlington` `UNAUTHORISED`

*Show a masked literal instead of the value*

Unknown: `276 North Drive`

*Field is masked as the unknown value (?)*

Progress®

© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

# Terminology for DDM

- Mask: P:, N:, L:, D:
- User-Defined Roles
- Authorization Tags

| | HR Manager | HR | Manager | Rest of all |
|---|---|---|---|---|
| Contact info | View | View | View | View |
| Leaves | View | View | View | Mask |
| Benefits | View | Mask | View | Mask |
| SSN | View | Mask | Mask | Mask |

- Authorization tag is a link between roles and
- masked fields
- Must begin with #DDM_See_
  - #DDM_See_Private
    - **SSN, D:**
  - #DDM_See_Protected_fldGrp1
    - **Leaves, L:9999**
  - #DDM_See_Protected_fldGrp2
    - **MedicalPlan N:, StockGrant D**:
- **HR**
  - #DDM_See_Protected_fldGrp1
- **Manager**
  - #DDM_See_Protected_fldGrp1
  - #DDM_See_Protected_fldGrp2
- **HRManager**
  - #DDM_See_Protected_fldGrp1
  - #DDM_See_Protected_fldGrp2
  - #DDM_See_Private

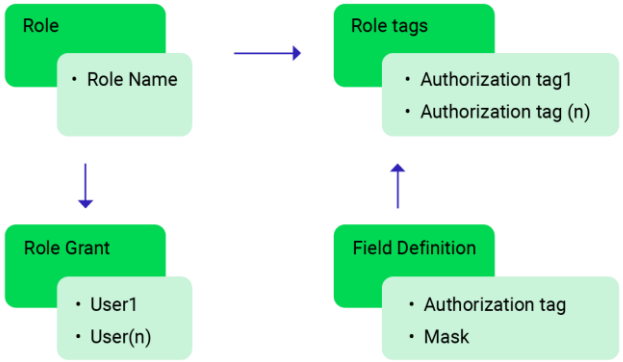
Progress®

© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

# Terminology for DDM

- Mask: P:, N:, L:, D:
- Authorization Tags
- User-Defined Roles

| | HR Manager | HR | Manager | Rest of all |
|---|---|---|---|---|
| Contact info | View | View | View | View |
| **Leaves** | **View** | **View** | **View** | **Mask** |
| **Benefits** | **View** | **Mask** | **View** | **Mask** |
| **SSN** | **View** | **Mask** | **Mask** | **Mask** |



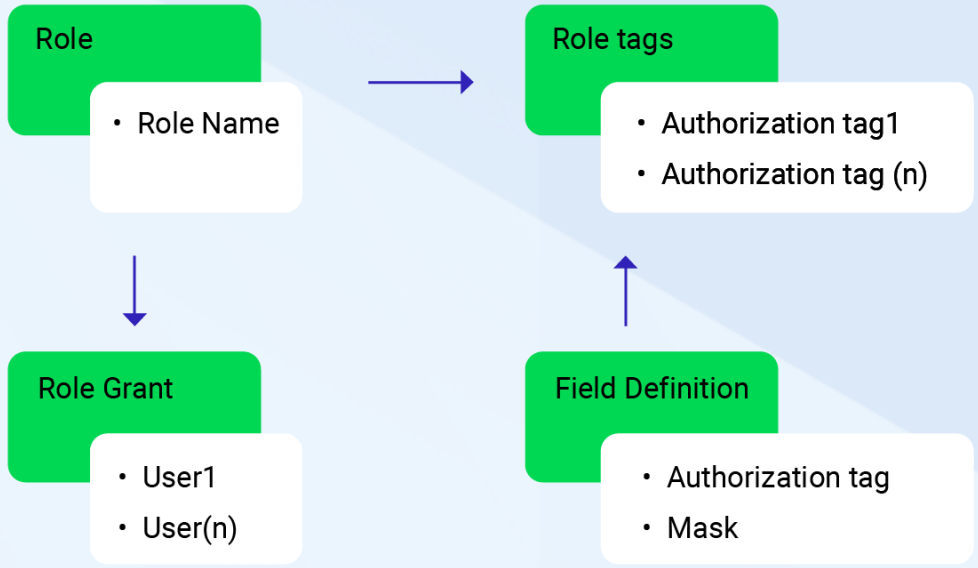

- Authorization tag is a link between roles and
- masked fields
- Must begin with #DDM_See_
  - #DDM_See_Private
    - **SSN, D:**
  - #DDM_See_Protected_fldGrp1
    - **Leaves, L:9999**
  - #DDM_See_Protected_fldGrp2
    - **MedicalPlan N:, StockGrant D**:
- **HR**
  - #DDM_See_Protected_fldGrp1
- **Manager**
  - #DDM_See_Protected_fldGrp1
  - #DDM_See_Protected_fldGrp2
- **HRManager**
  - #DDM_See_Protected_fldGrp1
  - #DDM_See_Protected_fldGrp2
  - #DDM_See_Private

Progress

© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

# Terminology for DDM

- Mask: P:, N:, L:, D:
- Authorization Tags
- User-Defined Roles
- DDM Administrator
  - Separation of concerns
  - Security Admin becomes DDM Admin if no user is granted a DDM Admin role




- Activate/Deactivate DDM
- Grant/Revoke Membership of User-defined DDM Roles
- Manage Authorization Tags
- Assign Authorization Tags and Mask to the Field

Progress®

© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

# DDM Security – Things to Know

By default, everyone is a DB Admin so everyone can change DDM settings

If DB Security Admins are set up, these users will default to control the DDM Administration

If separation of duties is required, a separate DDM Admin can be set by assigning this user to the _sys.ddm.admin role


© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

# What You Need for Dynamic Data Masking

- OpenEdge 12.8.3+ database with Advance Security License installed
- All clients need to be 12.8, older clients cannot connect once DDM is enabled
- A security administrator (optional but recommended)
- A DDM administrator (optional to provide separation of duties)
- A list of database fields that need to be masked by default
- Users that can unmask the fields

Progress®

© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

# DDM: OpenEdge 12.8

- New built-in role for DDM admin
  - _sys.ddm.admin
- New functionality added to PROUTIL utility
  - Deactivate keeps configurations in the system
  - Need to remove DDM configuration before disabling

```
proutil db-name –C enableddm

proutil db-name –C activateddm
                   [-U userid –P password]

proutil db-name –C deactivateddm
                   [-U userid –P password]

proutil db-name –C disableddm
                   [-U userid –P password]
```


© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

# DB Utilities for DDM Administration

## Enable DDM

**enableddm**
This sets the DDM feature bit in the database.
DDM will be inactive by default.
DDM can't be enabled if clients from a prior release are connected.
Requires Advanced Security license.

## Activate DDM

**activateddm**
Activating DDM notifies all connected clients that they must comply with the policies and masking rules.
Requires Advanced Security license.

## Deactivate DDM

**deactivateddm**
All connected clients will no longer honor the DDM policies that have been set up.
Any masking that has been set up will be ignored.
Doesn't require Advanced Security license but will need OpenEdge 12.8+.

## Disable DDM

All DDM user configuration information must be removed before running disableddm.
After disablement, a DB will revert to allow earlier OpenEdge clients to be able to connect that don't support masking.
Doesn't require Advanced Security license but does need OpenEdge 12.8+.

Progress®
© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

# DDM: OpenEdge 12.8

- IDataAdminService Interface to manage DDM
  - Roles
  - Authorization tags
  - Masks
- In the future tooling will be provided through the OpenEdge Command Center (OECC)

| |
|---|
| **Logical CreateRole (poRole AS IRole)** |
| Logical **UpdateRole** (poRole AS IRole) |
| Logical **DeleteRole** (roleName AS CHARACTER) |
| Logical **CreateAuthTag** (tag AS IAuthTag) |
| Logical **UpdateAuthTag** (tag AS IAuthTag) |
| Logical **DeleteAuthTag** (pcRoleName AS CHARACTER, pcAuthTag AS CHARACTER) |
| **GetAuthTags**() |
| Logical **setDDMConfig** (*tablename* AS CHARACTER, *fieldname* AS CHARACTER, *maskval* AS CHARACTER, *authtag* AS CHARACTER) |
| Logical **unsetDDMMask** (*tablename* AS character, *fieldname* AS character) |
| Logical **unsetDDMAuthTag** (*tablename* AS character, *fieldname* AS character) |
| **GetFieldDDMConfig** (input tablename AS character, input fieldname AS character, output maskval AS character, output authtag AS character) |


© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

# Configure DDM

© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

# Configure DDM

- **Enable DDM**

| | HR Manager | HR | Manager | Rest of all |
|---|---|---|---|---|
| Contact info | View | View | View | View |
| Leaves | View | View | View | Mask |
| Benefits | View | Mask | View | Mask |
| SSN | View | Mask | Mask | Mask |

**DB:** dbs2020 with SSN field in employee

**Users:** secadmin, ddmadmin, MrHRManager, MissHR, MissManager, RestOfWorld

```
proutil dbs2020 -C enableddm
```

Progress®

© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

# Configure DDM

- Enable DDM
- **Create DDM Admin with Grant Permissions**

| | HR Manager | HR | Manager | Rest of all |
|---|---|---|---|---|
| Contact info | View | View | View | View |
| Leaves | View | View | View | Mask |
| Benefits | View | Mask | View | Mask |
| SSN | View | Mask | Mask | Mask |

**DB:** dbs2020 with SSN field in employee

**Users:** secadmin, ddmadmin, MrHRManager, MissHR, MissManager, RestOfWorld

```
 VAR DataAdminService oDAS
...
oDAS             = NEW DataAdminService("dbs2020").
oRole            = oDAS:NewGrantedRole().
oRole:Role       = oDAS:GetRole("_sys.ddm.admin").
oUser            = oDAS:GetUser("ddmadmin").
oRole:Grantee    = oUser:Name.
oRole:CanGrant   = lGrantRights.
lResult          = oDAS:CreateGrantedRole(oRole).
...
```


© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

# Configure DDM

- Enable DDM
- Create DDM Admin with Grant Permissions
- **Create Roles**
  - **Log in as secadmin**

| | HR Manager | HR | Manager | Rest of all |
|---|---|---|---|---|
| Contact info | View | View | View | View |
| Leaves | View | View | View | Mask |
| Benefits | View | Mask | View | Mask |
| SSN | View | Mask | Mask | Mask |

**DB:** dbs2020 with SSN field in employee

**Users:** secadmin, ddmadmin, MrHRManager, MissHR, MissManager, RestOfWorld

```
...
VAR DataAdminService oDAS. VAR IRole oRole.
ASSIGN oDAS = NEW DataAdminService("dbs2020").

oRole              = oDAS:NewRole("HRManager").
oRole:Description  = "Manager in HR".
oRole:IsDDM        = true.
lResult            = oDAS:CreateRole(oRole).

DELETE OBJECT oDAS.
...
```


© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

# Configure DDM

- Enable DDM
- Create DDM Admin with Grant Permissions
- Create Roles
- **As DDM Admin:**
  - **Assign Tags**

| | HR Manager | HR | Manager | Rest of all |
|---|---|---|---|---|
| Contact info | View | View | View | View |
| Leaves | View | View | View | Mask |
| Benefits | View | Mask | View | Mask |
| SSN | View | Mask | Mask | Mask |

**DB:** dbs2020 with SSN field in employee

**Users:** secadmin, ddmadmin, MrHRManager, MissHR, MissManager, RestOfWorld

```
...
VAR DataAdminService oDAS. VAR IAuthTag oTag.
ASSIGN oDAS = NEW DataAdminService("dbs2020").

oTag            = service:NewAuthTag
                  ("#DDM_SEE_PrivateInfo").
oTag:RoleName   = service:GetRole("HRManager"):Name.
oTag:description = "Can see private info".
lRETURN           = service:CreateAuthTag(oTag).

DELETE OBJECT oDAS.
...
```


© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

# Configure DDM

- Enable DDM
- Create DDM Admin with Grant Permissions
- Create Roles
- **As DDM Admin:**
  - Assign Tags
  - **Assign Tags-Mask to Fields**

| | HR Manager | HR | Manager | Rest of all |
|---|---|---|---|---|
| Contact info | View | View | View | View |
| Leaves | View | View | View | Mask |
| Benefits | View | Mask | View | Mask |
| SSN | View | Mask | Mask | Mask |

**DB:** dbs2020 with SSN field in employee

**Users:** secadmin, ddmadmin, MrHRManager, MissHR, MissManager, RestOfWorld

```
...
VAR DataAdminService oDAS. VAR IAuthTag oTag.
ASSIGN oDAS = NEW DataAdminService("dbs2020").

lRETURN  = oDAS:setDDMConfig("employee",
                             "SSN",
                             "D:",
                             "#DDM_SEE_PrivateInfo").

DELETE OBJECT oDAS.
...
```

- #DDM_See_Private
  - SSN, D:

© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

# Configure DDM

- Enable DDM
- Create DDM Admin with Grant Permissions
- Create Roles
- **As DDM Admin:**
  - Assign Tags
  - Assign Tags-Mask to Fields
  - **Grant Roles to User**

| | HR Manager | HR | Manager | Rest of all |
|---|---|---|---|---|
| Contact info | View | View | View | View |
| Leaves | View | View | View | Mask |
| Benefits | View | Mask | View | Mask |
| SSN | View | Mask | Mask | Mask |

**DB:** dbs2020 with SSN field in employee

**Users:** secadmin, ddmadmin, MrHRManager, MissHR, MissManager, RestOfWorld

```
...
VAR DataAdminService oDAS.
ASSIGN oDAS = NEW DataAdminService("dbs2020").

oRole           = oDAS:NewGrantedRole().
oRole:Role      = oDAS:GetRole("HRManager").
oUser           = oDAS:GetUser("MrHRManager").
oRole:Grantee   = oUser:Name.
oRole:CanGrant = false.

lResult         = oDAS:CreateGrantedRole(oRole).
DELETE OBJECT oDAS.
...
```


© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

# Configure DDM

- Enable DDM
- Create DDM Admin with Grant Permissions
- Create Roles
- As DDM Admin:
  - Assign Tags
  - Assign Tags-Mask to Fields
  - Grant Roles to User
- **Activate DDM**

| | HR Manager | HR | Manager | Rest of all |
|---|---|---|---|---|
| Contact info | View | View | View | View |
| Leaves | View | View | View | Mask |
| Benefits | View | Mask | View | Mask |
| SSN | View | Mask | Mask | Mask |

**DB:** dbs2020 with SSN field in employee

**Users:** secadmin, ddmadmin, MrHRManager, MissHR, MissManager, RestOfWorld

```
proutil dbs2020 -C activateddm
```

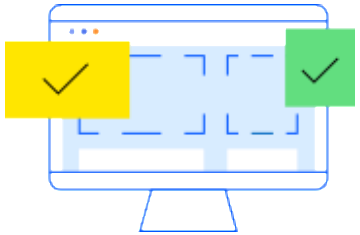

© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

# How It Works

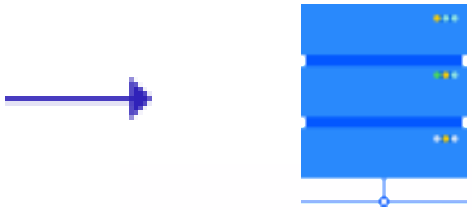
© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

# How It Works

```
FOR EACH EMPLOYEE BY Leaves:
DISPLAY FirstName Lastname
        Leaves.
END.
```



Client



Server

Database

| First Name | Last Name | Leaves |
|---|---|---|
| Emma | Brown | 9999 |
| Noah | Jones | 9999 |
| Olivia | Johnson | 9999 |
| Liam | Smith | 9999 |

| First Name | Last Name | Leaves |
|---|---|---|
| Emma | Brown | 10 |
| Noah | Jones | 8 |
| Olivia | Johnson | 4 |
| Liam | Smith | 1 |

| First Name | Last Name | Leaves |
|---|---|---|
| Liam | Smith | 1 |
| Noah | Jones | 8 |
| Emma | Brown | 10 |
| Olivia | Johnson | 4 |

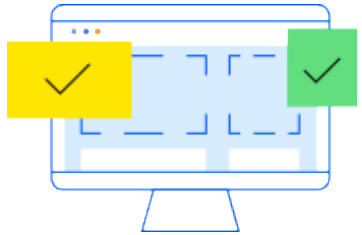
| First Name | Last Name | Leaves |
|---|---|---|
| Liam | Smith | 1 |
| Noah | Jones | 8 |
| Emma | Brown | 10 |
| Olivia | Johnson | 4 |

Masking is applied when data moves from `BUFFER` to the presentation layer.


© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

# How It Works

```
FOR EACH EMPLOYEE BY Leaves:
DISPLAY FirstName Lastname
        Leaves.
END.
```



Client

| First Name | Last Name | Leaves |
|---|---|---|
| Emma | Brown | 9999 |
| Noah | Jones | 9999 |
| Olivia | Johnson | 9999 |
| Liam | Smith | 9999 |

| First Name | Last Name | Leaves |
|---|---|---|
| Emma | Brown | 10 |
| Noah | Jones | 8 |
| Olivia | Johnson | 4 |
| Liam | Smith | 1 |

Masking is applied when data moves from `BUFFER` to the presentation layer.

- Masked field/column remains masked
  - Displayed on screen
  - Assigned to temp-table column
  - Exported to file
  - Referenced in conditional statement
  - Passed as Parameter
  - Assigned to program variable
- However, the query processing engine can always see the unmasked values


© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

# What Dynamic Data Masking Is Not

- Not a true security feature
- Not a method for encrypting data in the database
- Not a method for encrypting data over the network
- Not a tool to replicate databases and obfuscate at the database level
- Not a way of masking BLOBs or CLOBs
- Not a quick fix for regulatory compliance


© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

# OpenEdge 12.8: DDM DEMO

## Let’s See It in Action…

© 2023 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

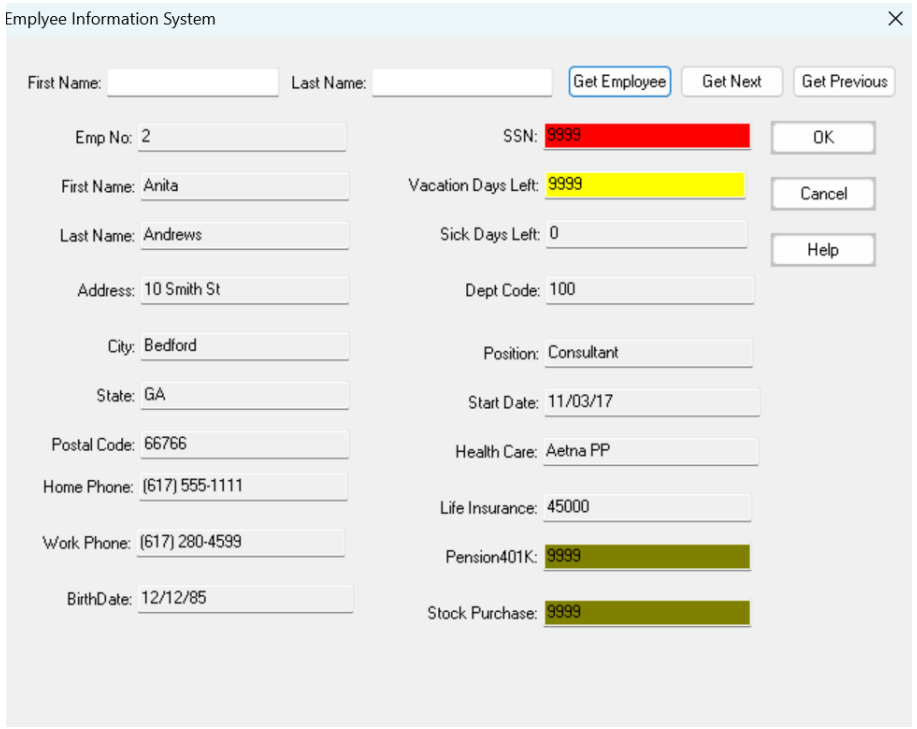
# Configure DDM

- Enable DDM
- Create DDM Admin with Grant Permissions
- Create Roles
- As DDM Admin:
  - Assign Tags
  - Assign Tags-Mask to Fields
  - Grant Roles to User
- Activate DDM

| | HR Manager | HR | Manager | Rest of all |
|---|---|---|---|---|
| Contact info | View | View | View | View |
| Leaves | View | View | View | Mask |
| Benefits | View | Mask | View | Mask |
| SSN | View | Mask | Mask | Mask |

**DB:** dbs2020 with SSN field in employee

**Users:** secadmin, ddmadmin, MrHRManager, MissHR, MissManager, RestOfWorld




© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

# Resources

| Content Name | Content Type | URL |
|---|---|---|
| Introduction to Dynamic Data Masking | OpenEdge Documentation | https://docs.progress.com/bundle/openedge-security-and-auditing/page/Introduction-to-Dynamic-Data-Masking.html |
| Dynamic data masking in OpenEdge SQL server | OpenEdge Documentation | https://docs.progress.com/zh-CN/bundle/openedge-sql-development/page/Dynamic-data-masking-in-OpenEdge-SQL-server.html |
| IDataAdminService methods for Dynamic Data Masking | OpenEdge Documentation | https://docs.progress.com/bundle/openedge-programming-interfaces/page/IDataAdminService-methods-for-Dynamic-Data-Masking.html |
| IDataAdminService examples for Dynamic Data Masking | OpenEdge Documentation | https://docs.progress.com/bundle/openedge-programming-interfaces/page/IDataAdminService-examples-for-Dynamic-Data-Masking.html |
| DataAdminService | OpenEdge Documentation | https://documentation.progress.com/output/oehttpclient/oe128/index.html?OpenEdge.DataAdmin.DataAdminService.html |

Progress®

© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

# Steps to Enable, Configure, Activate DDM

| Step | Code |
|---|---|
| 1. Get a database and start it | proserve sports2020 |
| 2. Enable Dynamic Data Masking | proutil sports2020 -C enableddm |
| 3. Add users (if not already present) | DBAdmin, DDMAdmin, MrHRManager, etc… |
| 4. Create a security user (optional but recommended) | Assign DBAdmin as the Security User |
| 5. Create a DDM Admin (optional) | Assign DDMAdmin as the DDM Admin |
| 6. Add field masking | Set the field masking method and assign the tag that the user must have to unmask the field |
| 7. Add DDM Role(s) | Create Roles for Employee Information System |
| 8. Add Tag to Role association | Allocate the tags used in the masking to the role |
| 9. Grant Role to user allowing field to be unmasked | Grant the User to the Role |
| 10. Activate Dynamic Data Masking | proutil sports2020 -C activateddm |


© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

# Questions?

© 2024 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved.

Progress® OpenEdge®

# News You Can Use


Progress®