



Simple Data Masking™ FAQ



Why risk using live data when de-identifying your records is simple?

Have your test and development teams been using live customer data? If so, you run the risk of incurring large fines for non-compliance with industry regulations, which state that all sensitive records must be de-identified for use in non-production environments.

Simple Data Masking™ is a fast, simple-to-use masking engine that enables users to de-identify and protect your sensitive data to ensure full regulatory compliance.

Simple Data Masking™ is a powerful, universal data masking engine that enables users to de-identify data for all major database types across multiple projects. Boasting a flexible approach to masking and de-identifying test data, Simple Data Masking™ can be installed as a stand-alone solution for small or medium-sized projects, or as part of our more holistic Enterprise Data Masking™ suite for larger projects.

As the name suggests, Simple Data Masking™ provides a simple-to-use data masking engine that is powered by the award-winning Datamaker™ tool. Simple Data Masking™ uses spread sheets to define and store masking rules, before masking them using the built-in, industrial strength masking algorithms, or calling out to your own procedures.

Each algorithm is fully automated, and applied across all data sources, tables and executions for consistent masking that ensures full referential integrity is maintained across all your projects. With Simple Data Masking™, you'll be using high-quality, fully compliant, meaningful test data within minutes!

What is data masking?

Data masking (sometimes referred to as de-identification, scrambling, obfuscation, or anonymization) is the process of masking sensitive or personally identifiable information (PII) within a database to ensure that it is secure for use in non-production environments.

In light of recent regulations and guidelines, such as the EU Data Protection Directive, and HIPAA and GLBA (USA), data masking has become standard industry best practice.



What types of system is Simple Data Masking™ suitable for?

Simple Data Masking™ is suitable for organizations with a need to quickly and easily de-identify or mask production data for use in non-production environments. Simple Data Masking™ can be used across projects of all sizes, with multiple projects requirements.

What does Simple Data Masking™ do?

Simple Data Masking™ offers all the functionality you need to provision fully compliant high-quality, meaningful test data, in one simple-to-use, industrial-strength solution.

Why should you invest in Simple Data Masking™?

In recent years, using masked and de-identified data in non-production environment has become standard industry practice. Not only is this demanded by industry regulations and guidelines, including the PCI DSS, HIPAA and GLBA (US) and EU Data Protection Directive, but using copies of live production databases has, in recent times, resulted in embarrassing, and preventable, data leaks. These leaks not only incur penalties from the regulators, but can damage credibility with customers and trading partners.

What data types does Simple Data Masking™ support?

Simple Data Masking™ supports all major database types, including:

- Oracle
- DB2
- SQL Server
- MySQL
- Sybase
- Ingres
- ODBC
- Flat files

How is the software installed and what are the system requirements?

- The software requires a JRE (Java Runtime Environment, Java 1.6 or higher) and will run on Windows, Linux, UNIX and Z/OS Platforms
- The masking rules are stored in spread sheets
- Standard seed tables are shipped and can be easily added.

How does Simple Data Masking™ work?

A series of intuitive and straightforward rules are defined to mask and anonymize the data.

The collection of rules includes:

- Seed tables
- Multi-table column seed tables
- Hashing
- Offsetting dates
- Substitution and replacements
- Credit Cards
- Phone numbers
- National ID numbers
- Random ranges
- Numeric variances
- Email addresses
- Any built-in SQL function
- etc

Simple to implement

Works for all database types

Works against any ODBC data source

You can mask consistently across different RDBMSs and databases

Auditing of old and new values

Provides multiple built-in routines to mask data

You can easily include your own custom masking routines

Allows the addition of your own seed tables to ensure data looks 'production like'

Standard seed tables include:

Names – First, Last, Male, Female and ethnic variations

Addresses – US, UK and International

Company names

etc