Security Best Practices

Datazen Enterprise Server

This document contains a list of recommendations for improving the security of your Datazen Enterprise Server environment. While following these recommendations does not guarantee freedom from security issues, these recommendations can significantly reduce your risk.

# Installation and Configuration

## Ensure the host machine is configured securely.

Many organizations have security policy in place to improve the security of servers in their environment. At a minimum, you should ensure that the server has all security updates applied, has up to date anti-virus software and that the local firewall is configured properly.

## Install the latest Datazen service packs.

The latest version of Datazen includes all the latest updates and should always be used.

## Install Web Applications and Core Service on separate machines.

By installing Datazen Enterprise Server Web Applications and Core Service on separate machines, the ability to compromise data residing in Core Service via an attack originating from the web is significantly reduced. Only install the required components on each machine, and consider installing Web Applications in the DMZ and other Datazen components in the internal network.

## Secure the instance id and encryption key.

During the initial installation of Core Service, a random instance id and encryption key are generated which are unique to your Datazen Enterprise Server environment. Secure these items carefully, as they could be maliciously used to gain access to various Datazen Enterprise Server services and/or decrypt the Core Service repository.

# Core Service

## Do not run Core Service as LocalSystem.

During the initial installation of Core Service you are prompted for the credentials to run the service as. Choose a local service account, and not LocalSystem. The service account requires the following rights and privileges:

* Modify files in the Datazen Enterprise Server installation target folder.
* Log on as a service.
* Back up files and directories.
* Replace a process-level token.
* Be a member of Performance Log Users group.

The Datazen Enterprise Server installer will configure the required security privileges for the chosen account. LocalSystem has privileges beyond what is required for Core Service operation, and can greatly increase risk should this service be compromised.

## Do not disable the account lockout feature.

The Datazen Enterprise Server account lockout feature restricts the number of authentication failures allowed before the account is administratively locked. If this feature is disabled the risk of a brute-force password attack is exposed.

## Only allow inbound traffic from other Datazen Enterprise Server services.

Core Service is exclusively utilized by other Datazen Enterprise Server services and Web Applications. Consider setting up a firewall security policy that only allows inbound traffic from addresses/ports running other Datazen Enterprise Server components. The default network ports required by Core Service are: TCP/28952 and TCP/28953.

## Provision an encrypted tunnel.

Although much of the traffic inbound to Core Service is encrypted, consider setting up an IPsec tunnel for use by the various server-side components of Datazen Enterprise Server. Use of an encrypted tunnel will greatly reduce the ability of malicious parties to eavesdrop on server-side network traffic.

## Restrict repository backup folder permissions.

When configuring the Core Service repository backup, ensure the target folder’s security permissions do not allow unnecessary access. The backup (although encrypted) contains sensitive information that should not be accessible to non-administrative users.

# Web Applications

## Install Web Applications in the DMZ.

Web Applications is the only component of the Datazen Enterprise Server product that features a public interface. Since no sensitive information is ever stored within Web Application state, it may be safely deployed to a DMZ. Other components of the Datazen Enterprise Server should be deployed to the secure internal network.

## Only allow required network traffic from the internal network.

Since Web Applications is the public interface of the Datazen Enterprise Server product it is important to only allow necessary network traffic to reach these machines, such as Remote Desktop traffic (for management purposes).

## Allow only HTTPS traffic from the public network.

Although Web Applications can be configured to respond to HTTP requests, it is strongly recommended that this functionality be relegated in favor of HTTPS.

## Do not modify IIS application pools identities or privileges.

Datazen Enterprise Server Web Applications run under three IIS applications pool identities: *Datazen.Server.ControlPanel*, *Datazen.Server.WebApi* and *Datazen.Server.Renderer*. These application pool identities are created and configured by the Datazen Enterprise Server installer with reduced security privileges. Granting excessive permissions to these application pool identities could increase the vulnerability to attacks via the Datazen Enterprise Server web interface.

# Data Acquisition Service

## Do not run Data Acquisition Service as LocalSystem.

During the initial installation of Data Acquisition Service you are prompted for the credentials to run the service as. Choose a local service account, and not LocalSystem. The service account requires the following rights and privileges:

* Modify files in the Datazen Enterprise Server installation target folder.
* Log on as a service.
* Be a member of Performance Log Users group.

The Datazen Enterprise Server installer will configure the required security privileges for the account. LocalSystem has privileges beyond what is required for Data Acquisition Service operation, and can greatly increase risk should this service be compromised.

# Authentication

## Avoid using default authentication.

If possible, avoid using Datazen Enterprise Server default authentication in favour of one of the other supported authentication mechanisms. The default authentication provider stores hashed user credentials within the Core Repository and if compromised, could potentially be used as an attack vector.

If all of the Datazen Enterprise Server users have Active Directory accounts, and the Active Directory environment is accessible to the Datazen Core Service (e.g. the Core Service machine is a domain member, or an Active Directory catalog can be queried via LDAP) consider using Active Directory authentication mode.

If all of the Datazen Enterprise Server users can utilize an existing Active Directory Federation Service environment, consider using ADFS authentication mode.

# Users and Hubs

## Configure BI hubs to adhere to organizational structure.

From a security standpoint, Datazen Enterprise Server BI hubs should reflect your organizational structure. Although Datazen Enterprise Server users can be placed into multiple BI hubs, members cannot view or interact with dashboards or data residing in BI hubs where they are not members.

## Restrict membership of the hub *Owner* role.

*Owners* have special privileges within a BI hub, such as creating and editing data connections and views, and managing membership for the hub and user groups contained within the BI hub. Only allow users who should have these elevated responsibilities to be in the *Owner* role.

# Data Connections

## Only use encrypted connections.

If the data provider allows it, always use an encrypted connection when creating a data connection. Connecting to a back-end data source with an unencrypted connection could expose user credentials to malicious parties.

## Ensure SSAS back-end servers running IIS/msmdpump.dll are secured with SSL.

When configuring SSAS data connections to back-end servers running IIS/msmdpump.dll, make sure the endpoint is secured with SSL. Connecting to SSAS data sources that are not configured in this way could expose user credentials to malicious parties.

## Lock down data providers.

If the Datazen Enterprise Server data connection requirements are well known, the server administrator should lock down the set available of data providers so that data connection authors may only select a provider from this approved set.