Using Two-Factor Authentication to Connect to a Kerberos-enabled Informatica Domain
Abstract
Two-factor authentication (2FA), utilizing smart cards or USB tokens, is a popular network security mechanism. This article explains how two-factor authentication works in an Informatica domain configured to use Kerberos authentication. The information in the article might also be useful when troubleshooting authentication issues.

Supported Versions
- Informatica Big Data Management 9.6.1, 10.0, 10.1
- Informatica Data Quality 9.6.1, 10.0, 10.1
- Informatica Data Services 9.6.1, 10.0, 10.1
- Informatica PowerCenter 9.6.1, 10.0, 10.1

Table of Contents
Overview ............................................................... 2
Requirements ........................................................... 2
How It Works ............................................................ 3
View the Kerberos Tickets Created for a User ....................... 4
Increase the Kerberos Buffer Size to Accommodate Large Tokens 5

Overview
You must first establish connectivity using two-factor authentication (2FA) to your internal network utilizing smart cards or USB tokens. After an Informatica client user logs in to the network using two-factor authentication, Informatica uses the Kerberos authentication protocol to enable the user to access assets such as nodes and services within the Informatica domain hosted on supported platforms as per the PAM.

The following Informatica clients on a 2FA enabled Windows server can connect to a Kerberos-enabled Informatica domain:
- Thick clients such as the PowerCenter Client and Informatica Developer (the Developer tool)
- Web clients such as Informatica Administrator (the Administrator tool)
- Command-line clients such as infacmd, pmcmd, and pmrep

Kerberos tickets enable Informatica client users to authenticate with Informatica domain assets, without requiring users to log in to each asset. You can view the Kerberos tickets generated for client users to help troubleshoot issues. You can also increase the Kerberos token buffer size if needed to resolve authentication failures.

Requirements
Validate the following requirements to ensure that two-factor authentication is done before connecting to the Informatica domain:
- Verify that the Windows server hosting the Informatica client tools is configured to use two-factor authentication.
- Confirm that the network is configured to use Microsoft Active Directory, which maintains user account information required by Kerberos.
• Ensure that the Informatica domain is configured to use Kerberos authentication. You can enable Kerberos authentication during the Informatica domain installation, or use the Informatica command line programs to configure it post-installation.


**Note:** Informatica does not support cross-realm or multi-realm Kerberos authentication. The Informatica domain nodes, the Kerberos authentication server, and the computers hosting Informatica clients must all be in the same Kerberos realm.

### How It Works

The Informatica two-factor authentication implementation uses Kerberos tickets to authenticate Informatica client users on assets such as nodes and services within the Informatica domain.

The following outline describes the basic Kerberos authentication flow:

• An Informatica client user logs in to a network computer hosting an Informatica client using a device such as a smart card or a USB token.

• The login request is directed to the Authentication Server, a component of the Kerberos Key Distribution Center (KDC). The KDC is a network service with access to user account information that runs on each domain controller within the Active Directory domain.

![Diagram of Kerberos authentication flow]

- User logs into network through an Informatica client host. A TGT is created on the client host.
- User attempts to access an Informatica service via the client. The TGT is used to create a service ticket for the service and the domain node it is running on.
- The service ticket is cached on the client host. User is now able to access the Informatica service without having to log in.
- The Authentication Server creates a Kerberos token called a Ticket-Granting-Ticket (TGT) on the user’s computer.
The user attempts to access an asset within the Informatica domain through an Informatica client.

Informatica and the Kerberos libraries use the TGT to request a service ticket and session key for the requested domain asset from the Ticket Granting Server, which also runs within the KDC.

For example, if the user accesses a PowerCenter Repository Service from the PowerCenter Client, the TGT requests a service ticket for the node the PowerCenter Repository Service is running on. The TGT also requests a service ticket for the PowerCenter Repository Service.

The service ticket is cached on the computer hosting the Informatica client, enabling the client to use the ticket as long as it remains valid. If the user shuts down and then restarts the Informatica client, the client reuses the same ticket to access assets within the Informatica domain.

Forwardable and Renewable Tickets

The Ticket Flags field notes any Kerberos ticket flags set on the ticket. If a TGT or service ticket is flagged as renewable, the Informatica client can renew ticket at any point during the login session, without requiring the user to provide login credentials.

If a ticket is flagged as forwardable, Kerberos can use it to authenticate the user on a remote server, and enable the user to run an Informatica client on that server. For example, if the user wants to use the Secure Socket Shell (SSH) protocol to run the pmcmd command-line client on a remote server, Kerberos requests a service ticket for the remote server on the user's computer. Kerberos also forwards the original TGT to the remote server, so new service tickets can be created on the remote server.

The user is therefore able to access Informatica domain assets from the Informatica client running on the remote server, without having to log in on the remote server.

The following image shows the output of the Windows klist command, which lists details for the Kerberos tickets cached on an Informatica client user's computer. The krbtgt in the service name identifies the ticket shown as a TGT. The Ticket Flags field indicates that the ticket is both forwardable and renewable.

![Kerberos Tickets Output](image)

View the Kerberos Tickets Created for a User

You can use the Windows klist command to view the cached Kerberos ticket-granting-tickets and service tickets created for an Informatica client user. You might want to view tickets when trying to troubleshoot authentication issues. At minimum, it can be used to verify that a Kerberos ticket has been issued to the user.

To view the tickets created for a user on a computer hosting an Informatica client, type klist at the Windows command prompt. This the default option for the command, and returns all cached Kerberos tickets for network services the user has authenticated with.
Increase the Kerberos Buffer Size to Accommodate Large Tokens

You can increase the Kerberos buffer size on computers hosting Informatica clients if large tokens cause user authentication issues.

Depending on the Windows network configuration, Kerberos tickets created for a user may include Privilege Account Certificate (PAC) information. The PAC structure contains such data such as the user's security identifiers, group membership, user profile information, and password credentials. Depending on the amount of data stored, the PAC might make Kerberos tokens larger than the default allocated buffer size, resulting in authentication failures.

You can increase the Kerberos buffer size by adding the following value to the HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Control\Lsa\Kerberos\Parameters registry key on computers hosting Informatica clients:

- Entry: MaxTokenSize
- Type: REG_DWORD
- Base: Decimal
- Data: 48000

Author

Dan Hynes
Principal Technical Writer